One Identity Manager 9.1

Administrationshandbuch für die Anbindung kundendefinierter Zielsysteme

Legende

WARNUNG: Das Symbol WARNUNG weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.

VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

One Identity Manager Administrationshandbuch für die Anbindung kundendefinierter Zielsysteme
Aktualisiert - 19. September 2022, 13:02 Uhr

Die aktuellsten Versionen der Produktdokumentation finden Sie unter One Identity Manager Dokumentation.

Inhalt

1

Verwalten kundendefinierter Zielsysteme

Im One Identity Manager können neben den direkt unterstützten Zielsystemen auch eigene Anwendungen, wie beispielsweise eine Telefonanlage, abgebildet werden. Um diese Zielsysteme mit dem One Identity Manager zu verwalten, erstellen Sie Containerstrukturen, Benutzerkonten, Gruppen und Systemberechtigungen. Gruppen und Systemberechtigungen bilden die Objekte ab, über die im Zielsystem der Zugriff auf die Zielsystemressourcen gesteuert wird.

HINWEIS: Voraussetzung für die Verwaltung kundendefinierter Zielsysteme im One Identity Manager ist die Installation des Zielsystem Basismoduls. Ausführliche Informationen zur Installation finden Sie im *One Identity Manager Installationshandbuch.*

Die One Identity Manager Bestandteile für die Verwaltung von kundendefinierten Zielsystemen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | UNS** aktiviert ist.

- Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.

  HINWEIS:Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.

Um Daten zwischen dem Zielsystem und der One Identity Manager-Datenbank auszutauschen, definieren Sie unternehmensspezifische Prozesse. Der One Identity Manager bietet verschiedene Möglichkeiten der Datenübernahme an.

- Für die Provisionierung der Daten stellt der One Identity Manager in der Standardinstallation vordefinierte Prozesse bereit. Die Prozesse verwenden Skripte zur Provisionierung der Daten. Da jedes kundendefinierte Zielsystem eine andere Abbildung der Daten erfordert, muss die Provisionierung der Daten aus dem One

Identity Manager in das kundendefinierte Zielsystem angepasst werden. Weitere Informationen finden Sie unter Einrichten der Skript-gesteuerten Provisionierung der Daten in ein kundendefiniertes Zielsystem auf Seite 12.

- Alternativ zur Skript-gesteuerten Synchronisation können Sie eine Synchronisation mittels CSV Konnektor einrichten. Dies erfordert umfangreiche kundenspezifische Anpassungen. Ausführliche Informationen dazu finden Sie im *One Identity Manager Anwenderhandbuch für den CSV Konnektor*.
- Mit dem Programm Data Import bietet der One Identity Manager einen einfache Möglichkeit für den Datenimport aus anderen Systemen. Das Programm unterstützt Importe aus `.csv`-Dateien und direkte Importe aus anderen Datenbanksystemen. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

One Identity Manager Benutzer für die Verwaltung von kundendefinierten Zielsystemen

In die Einrichtung und Verwaltung von kundendefinierten Zielsystemen sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	Die Zielsystemadministratoren müssen der Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen. • Legen die Zielsystemverantwortlichen fest. • Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein. • Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen. • Berechtigen weitere Personen als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der

Benutzer	Aufgaben
	Anwendungsrolle **Zielsysteme | Kundendefinierte Zielsysteme** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen und Systemberechtigungen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne.

Benutzer	Aufgaben
	• Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.
Administratoren für den IT Shop	Die Administratoren müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an IT Shop-Strukturen zu. • Weisen Systemberechtigungen an IT Shop-Strukturen zu.
Administratoren für Organisationen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Organisationen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an Abteilungen, Kostenstellen und Standorte zu. • Weisen Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zu.
Administratoren für Geschäftsrollen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an Geschäftsrollen zu. • Weisen Systemberechtigungen an Geschäftsrollen zu.

Konfigurationsparameter für die Verwaltung von kundendefinierten Zielsystemen

Über Konfigurationsparameter konfigurieren Sie die Grundeinstellungen zum Systemverhalten. Der One Identity Manager stellt für verschiedene Konfigurationsparameter Standardeinstellungen zur Verfügung. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.

Die Konfigurationsparameter sind in den One Identity Manager Modulen definiert. Jedes One Identity Manager Modul kann zusätzliche Konfigurationsparameter installieren. Einen

Überblick über alle Konfigurationsparameter finden Sie im Designer in der Kategorie **Basisdaten > Allgemein > Konfigurationsparameter**.

Weitere Informationen finden Sie unter Konfigurationsparameter für die Verwaltung kundendefinierter Zielsysteme auf Seite 154.

Einrichten der Skript-gesteuerten Provisionierung der Daten in ein kundendefiniertes Zielsystem

Für die Provisionierung der Daten stellt der One Identity Manager in der Standardinstallation vordefinierte Prozesse bereit. Die Prozesse verwenden Skripte zur Provisionierung der Daten. Da jedes kundendefinierte Zielsystem eine andere Abbildung der Daten erfordert, muss die Provisionierung der Daten aus dem One Identity Manager in das kundendefinierte Zielsystem angepasst werden.

Die Verarbeitung der Prozesse erfolgt durch den generischen Webservice. Ausführliche Informationen zum generischen Webserviceaufruf finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um dieses Provisionierungsverfahren zu nutzen, sind die folgenden Schritte erforderlich:

- Erstellen der Skripte für die Provisionierung

  Die Provisionierung der Daten aus dem One Identity Manager in ein kundendefiniertes Zielsystem erfolgt über Skripte. Diese müssen für jedes Zielsystem erstellt werden. Weitere Informationen finden Sie unter Erstellen der Skripte für die Provisionierung der Daten in ein kundendefiniertes Zielsystem auf Seite 13.

- Bereitstellen eines Servers für die Provisionierung

  Auf dem Server muss der One Identity Manager Service installiert, konfiguriert und gestartet sein. Der Server muss im One Identity Manager bekannt sein und am Zielsystem als Synchronisationsserver eingetragen werden. Weitere Informationen finden Sie unter Jobserver für die Provisionierung der Daten in ein kundendefiniertes Zielsystem auf Seite 14.

- Einrichten des kundendefinierten Zielsystems in der One Identity Manager-Datenbank und anpassen der Synchronisationsmethode in der One Identity Manager-Datenbank.

  Wählen Sie die Synchronisationsmethode **Synchronisation per Skript**. Weitere Informationen finden Sie unter Kennungen für kundendefinierte Zielsysteme auf Seite 108.

TIPP: Alternativ zur Skript-gesteuerten Synchronisation können Sie eine Synchronisation mittels CSV Konnektor einrichten. Dies erfordert umfangreiche kundenspezifische Anpassungen. Ausführliche Informationen dazu finden Sie im *One Identity Manager Anwenderhandbuch für den CSV Konnektor.*

Erstellen der Skripte für die Provisionierung der Daten in ein kundendefiniertes Zielsystem

In der Standardinstallation des One Identity Manager werden für die Tabellen, die zur Abbildung kundendefinierter Zielsysteme benutzt werden, bereits Prozesse für die Standardereignisse (Insert, Update, Delete) zur Verfügung gestellt.

Die Prozesse verwenden Skripte zur Provisionierung der Daten. Da jedes kundendefinierte Zielsystem eine andere Abbildung der Daten erfordert, müssen die Skripte an das kundendefinierte Zielsystem angepasst werden.

Erstellen Sie kundenspezifische Skripte für Ihr Zielsystem. Als Vorlage für die Erstellung kundenspezifischer Skripte können Sie das Skript `TSB_Uns_Generic_Templates` verwenden.

Die Prozesse erwarten innerhalb der Skripte Funktionen, die nach folgendem Schema benannt sind:

`<Kundenpräfix>_<Tabelle>_<Ident_UNSRoot>_<Ereignis>`

Beispiel: Einfügen von Benutzerkonten in das kundendefinierte Zielsystem **Telefonanlage**

`CCC_UNSAccountB_Telefonanlage_Insert`

WICHTIG: Enthält ihr Zielsystem einen Bindestrich (**-**) im Namen, müssen Sie diesen in den Skriptfunktionen im Bestandteil `<Ident_UNSRoot>` entfernen. Anderenfalls können Fehler in der Skriptverarbeitung auftreten.

Die Objekte der kundendefinierten Zielsysteme werden in den folgenden Tabellen des One Identity Manager Schemas abgebildet.

Tabelle 2: Tabellen des One Identity Manager Schemas zur Abbildung kundendefinierter Zielsysteme

Tabelle	Beschreibung
UNSAccountB	Abbildung der Benutzerkonten.
UNSAccountBHasUNSGroupB	Zuweisungen von Gruppen zu Benutzerkonten.
UNSAccountBHasUNSGroupB1, UNSAccountBHasUNSGroupB2, UNSAccountBHasUNSGroupB3	Zuweisungen von Systemberechtigungen zu Benutzerkonten.
UNSAccountBHasUNSItemB	Zuweisungen von Berechtigungselementen zu Benutzerkonten.

Tabelle	Beschreibung
UNSAccountBInUNSGroupB	Zuweisungen von Benutzerkonten zu Gruppen.
UNSAccountBInUNSGroupB1, UNSAccountBInUNSGroupB2, UNSAccountBInUNSGroupB3	Zuweisungen von Benutzerkonten zu Systemberechtigungen.
UNSContainerB	Abbildung der Containerstruktur.
UNSGroupB	Abbildung der Gruppen.
UNSGroupB1, UNSGroupB2, UNSGroupB3	Abbildung weiterer Systemberechtigungen.
UNSGroupBHasUnsItemB	Zuweisungen von Berechtigungselementen zu Gruppen.
UNSGroupBInUNSGroupB	Zuweisungen von Gruppen zu Gruppen (Gruppenhierarchie).
UNSGroupB1InUNSGroupB1, UNSGroupB1InUNSGroupB2, UNSGroupB1InUNSGroupB3	Zuweisungen von Systemberechtigungen an Systemberechtigungen (Hierarchie der Systemberechtigungen).
UNSItemB	Abbildung von zusätzlichen Berechtigungselementen.
UNSRootB	Basis zur Abbildung des kundendefinierten Zielsystems.

Jobserver für die Provisionierung der Daten in ein kundendefiniertes Zielsystem

Für jedes kundendefinierte Zielsystem muss ein Server definiert werden, der alle Aktionen des One Identity Manager Service ausführt, die für die Provisionierung von Zielsystemobjekten erforderlich sind. Ausführliche Informationen zur Installation und Konfiguration des One Identity Manager Service finden Sie im *One Identity Manager Installationshandbuch*.

Um einen Server einzurichten

1. Stellen Sie einen Server bereit, auf dem der One Identity Manager Service installiert ist.
2. Erstellen Sie im Manager einen Eintrag für den Jobserver.

1. Wählen Sie die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Server**.
2. Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten für den Jobserver.
4. Speichern Sie die Änderungen.

3. Tragen Sie den Server am kundendefinierten Zielsystem als Synchronisationsserver ein.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Jobserver auf Seite 15
- Datensynchronisation für kundendefinierte Zielsysteme anpassen auf Seite 112

Allgemeine Stammdaten für Jobserver

HINWEIS: Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** zur Verfügung.

HINWEIS: Abhängig von den installierten Modulen können weitere Eigenschaften verfügbar sein.

Tabelle 3: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Syntax: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Zielsystem	Zielsystem des Computerkontos.
Sprachkultur	Sprache des Servers.
Server ist Cluster	Gibt an, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Quellserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme `Robocopy` und `rsync`

Eigenschaft	Bedeutung
	unterstützt. Wird kein Verfahren angegeben, ermittelt der One Identity Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausgeführt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm `Robocopy` und zwischen Servern mit einem Linux Betriebssystem mit dem Programm `rsync`. Unterscheiden sich die Betriebssysteme des Quellservers und des Zielservers, so ist für eine erfolgreiche Replikation die Angabe der zulässigen Kopierverfahren zwingend erforderlich. Es wird das Kopierverfahren eingesetzt, das beide Server unterstützen.
Kopierverfahren (Zielserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden. Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Mit dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des

Eigenschaft	Bedeutung
	Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	Gibt an, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur `QBM_PJobQueueLoad` aktiviert, sobald die Queue das erste Mal angefragt wird. Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Gibt an, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen Berechtigungen im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Pausiert wegen Nicht-verfügbarkeit eines Zielsystems	Gibt an, ob die Verarbeitung von Aufträgen für diese Queue angehalten wurde, weil das Zielsystem, für den dieser Jobserver der Synchronisationsserver ist, vorübergehend nicht erreichbar ist. Sobald das Zielsystem wieder erreichbar ist, wird die Verarbeitung gestartet und alle anstehenden Aufträge werden ausgeführt. Ausführliche Informationen zum Offline-Modus finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
Kein automatisches Softwareupdate	Gibt an, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Gibt an, ob gerade eine Softwareaktualisierung ausgeführt wird.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 18

Festlegen der Serverfunktionen

HINWEIS: Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** zur Verfügung.

HINWEIS: Abhängig von den installierten Modulen können weitere Serverfunktionen verfügbar sein.

Tabelle 4: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
CSV Konnektor	Server, auf dem der CSV Konnektor für die Synchronisation installiert ist.
Domänen-Controller	Active Directory Domänen-Controller. Server, die nicht als Domänen-Controller gekennzeichnet sind, werden als Memberserver betrachtet.
Druckserver	Server, der als Druckserver arbeitet.
Generischer Server	Server für die generische Synchronisation mit einem kundendefinierten Zielsystem.
Homeserver	Server zur Anlage von Homeverzeichnissen für Benutzerkonten.
Aktualisierungsserver	Der Server führt die automatische Softwareaktualisierung aller anderen Server aus. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Der Server kann SQL Aufträge ausführen. Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.
SQL Ausführungsserver	Der Server kann SQL Aufträge ausführen. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente `ScriptComponent` verarbeiten.
Generischer Datenbankkonnektor	Der Server kann sich mit einer ADO.Net Datenbank verbinden.
One Identity Manager-Datenbankkonnektor	Server, auf dem der One Identity Manager Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem

Serverfunktion	Anmerkungen
	Zielsystem One Identity Manager aus.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
Primärer Domänen-Controller	Primärer Domänen-Controller.
Profilserver	Server für die Einrichtung von Profilverzeichnissen für Benutzerkonten.
SAM Synchronisationsserver	Server für die Synchronisation mit einem SMB-basierten Zielsystem.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
Standard Berichtserver	Server, auf dem die Berichte generiert werden.
Windows PowerShell Konnektor	Der Server kann Windows PowerShell Version 3.0 oder neuer ausführen.

Nachbehandlung ausstehender Objekte

Objekte aus kundendefinierten Zielsystemen können durch unternehmensspezifisch definierte Prozesse regelmäßig in die One Identity Manager-Datenbank eingelesen werden. Dabei haben Sie die Möglichkeit, Objekte, die im Zielsystem nicht vorhanden sind, entweder direkt in der One Identity Manager-Datenbank zu löschen oder als ausstehend zu markieren. Ausführliche Informationen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Objekte, die im Zielsystem nicht vorhanden sind, können bei der Synchronisation in den One Identity Manager als ausstehend gekennzeichnet werden. Damit kann verhindert werden, dass Objekte aufgrund einer fehlerhaften Datensituation oder einer fehlerhaften Synchronisationskonfiguration gelöscht werden.

Ausstehende Objekte

- können im One Identity Manager nicht bearbeitet werden,
- werden bei jeder weiteren Synchronisation ignoriert,
- werden bei der Vererbungsberechnung ignoriert.

Das heißt, sämtliche Mitgliedschaften und Zuweisungen bleiben solange erhalten, bis die ausstehenden Objekte nachbearbeitet wurden.

Führen Sie dafür einen Zielsystemabgleich durch.

Um die Nachbehandlung ausstehender Objekte zu ermöglichen

- Konfigurieren Sie am Zielsystemtyp des zu synchronisierende Zielsystems den Zielsystemabgleich.

Verwandte Themen

- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 20
- Zielsystemtypen für kundendefinierte Zielsysteme auf Seite 149
- Ausstehende Objekte nachbehandeln auf Seite 21

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen

Um ausstehende Objekte nachbehandeln zu können, weisen Sie die Tabellen, die ausstehende Objekte enthalten können, dem Zielsystemtyp des kundendefinierten Zielsystems zu. Legen Sie die Tabellen fest, für die ausstehende Objekte in der Nachbehandlung in das Zielsystem publiziert werden dürfen.

Um Tabellen in den Zielsystemabgleich aufzunehmen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp des kundendefinierten Zielsystems.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Tabellen zu, für die Sie ausstehende Objekte behandeln möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die Tabellen, für die ausstehende Objekte in das Zielsystem publiziert werden dürfen und aktivieren Sie die Option **Publizierbar**.
8. Speichern Sie die Änderungen.

Um ausstehende Objekte publizieren zu können

1. Erstellen Sie Prozesse, welche die Provisionierung der Objekte ausführen, für:
   - einfache Tabellen
   - Zuordnungstabellen, die Zusatzinformationen enthalten, wie beispielsweise ein Gültig-von-Datum

   Verwenden Sie die Prozessfunktion `AdHocProjection` der Prozesskomponente `ProjectorComponent`.

Ausführliche Informationen zum Definieren von Prozessen finden Sie im *One Identity Manager Konfigurationshandbuch*.

2. Erstellen Sie das Ereignis `HandleOutstanding` für diese Prozesse.

Für Mitgliedschaften, die in einfachen Zuordnungstabellen abgebildet sind, wird beim Publizieren das **Änderungsdatum für Abhängigkeiten** (Spalte `XDateSubItem`) an der Basistabelle der Zuordnung geändert. Dadurch wird der Standard-Update-Prozess ausgelöst, der für diese Basistabelle eingerichtet ist. Ausführliche Informationen zur Kennzeichnung der Änderung von Mitgliedschaften finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Weitere Informationen finden Sie unter Einrichten der Skript-gesteuerten Provisionierung der Daten in ein kundendefiniertes Zielsystem auf Seite 12.

HINWEIS: Wenn Sie den CSV Konnektor zur Provisionierung nutzen, sorgen Sie dafür, dass der CSV Konnektor schreibend auf die CSV-Dateien zugreifen kann. Das heißt, an der Zielsystemverbindung ist die Option **Verbindung darf nur gelesen werden** deaktiviert. Ausführliche Informationen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Ausstehende Objekte nachbehandeln

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Zielsystemabgleich: <Zielsystemtyp>**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp zugewiesen sind.

2. Öffnen Sie auf dem Formular **Zielsystemabgleich**, in der Spalte **Tabelle/Objekt** den Knoten der Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

   Es werden alle Objekte angezeigt, die als ausstehend markiert sind. Die Spalten **Letzter Protokolleintrag** und **Letzte ausgeführte Methode** zeigen den Zeitpunkt für den letzten Eintrag im Synchronisationsprotokoll und die dabei ausgeführte Verarbeitungsmethode. Der Eintrag **Kein Protokoll verfügbar** hat folgende Bedeutungen:

   - Das Synchronisationsprotokoll wurde bereits gelöscht.

     - ODER -

   - Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.

     Bei der Synchronisation wird das Basisobjekt der Zuordnung aktualisiert. Dafür erscheint ein Eintrag im Synchronisationsprotokoll. Der Eintrag in der Zuordnungstabelle wird als ausstehend markiert, es gibt jedoch keinen Eintrag im Synchronisationsprotokoll.

   - Im Zielsystem wurde ein Objekt gelöscht, das eine Mitgliederliste enthält.

Bei der Synchronisation werden das Objekt und alle zugehörigen Einträge in Zuordnungstabellen als ausstehend markiert. Ein Eintrag im Synchronisationsprotokoll erscheint jedoch nur für das gelöschte Objekt.

TIPP:

Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

1. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.
2. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.

3. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.
4. Klicken Sie in der Formularsymbolleiste eins der folgenden Symbole, um die jeweilige Methode auszuführen.

Tabelle 5: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Es wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: • Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen. • Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen.
	Zurücksetzen	Die Markierung **Ausstehend** wird für das Objekt entfernt.

5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

HINWEIS: Standardmäßig werden die ausgewählten Objekte parallel verarbeitet. Damit wird die Ausführung der ausgewählten Methode beschleunigt. Wenn bei der Verarbeitung ein Fehler auftritt, wird die Aktion abgebrochen und alle Änderungen werden rückgängig gemacht.

Um den Fehler zu lokalisieren, muss die Massenverarbeitung der Objekte deaktiviert werden. Die Objekte werden damit nacheinander verarbeitet. Das fehlerhafte Objekt wird

in der Fehlermeldung benannt. Alle Änderungen, die bis zum Auftreten des Fehlers vorgenommen wurden, werden gespeichert.

Um die Massenverarbeitung zu deaktivieren

- Deaktivieren Sie in der Formularsymbolleiste das Symbol  .

Verwandte Themen

- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 20

Managen von Benutzerkonten und Personen

Zentraler Bestandteil des One Identity Manager ist die Abbildung von Personen mit ihren Stammdaten sowie den Berechtigungen, über die sie in verschiedenen Zielsystemen verfügen. Zu diesem Zweck können Informationen über Benutzerkonten und Berechtigungen aus den Zielsystemen in die One Identity Manager-Datenbank eingelesen und mit den Personen verbunden werden. Für jede Person kann damit ein Überblick über ihre Berechtigungen in allen angebundenen Zielsystemen gewonnen werden. Der One Identity Manager bietet die Möglichkeit Benutzerkonten und ihre Berechtigungen zu verwalten. Änderungen können in die Zielsysteme provisioniert werden. Die Personen werden so entsprechend ihrer Funktion mit den benötigten Berechtigungen in den angebundenen Zielsystemen versorgt. Regelmäßige Synchronisationsprozesse halten die Daten zwischen den Zielsystemen und der One Identity Manager-Datenbank konsistent.

Da die Anforderungen von Unternehmen zu Unternehmen unterschiedlich sind, bietet der One Identity Manager verschiedene Verfahren zur Versorgung einer Person mit den benötigten Benutzerkonten an. Der One Identity Manager unterstützt die folgenden Vorgehensweisen, um Personen und ihre Benutzerkonten zu verknüpfen:

- Personen erhalten ihre Benutzerkonten automatisch über Kontendefinitionen.

  Hat eine Person noch kein Benutzerkonto in einem Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Person über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

  Wenn Sie Benutzerkonten über Kontendefinitionen verwalten, können Sie das Verhalten von Benutzerkonten beim Deaktivieren oder Löschen von Personen festlegen.
- Beim Einfügen eines Benutzerkontos wird automatisch eine vorhandene Person zugeordnet oder im Bedarfsfall eine neue Person erstellt. Dabei werden die Personenstammdaten anhand vorhandener Benutzerkontenstammdaten erzeugt. Dieser Mechanismus kann eingesetzt werden, wenn ein neues Benutzerkonto manuell oder durch eine Synchronisation erstellt wird. Dieses Vorgehen ist jedoch nicht das Standardverfahren für den One Identity Manager. Für die automatische Personenzuordnung definieren Sie Kriterien, anhand derer die Personen ermittelt werden sollen.

- Personen und Benutzerkonten können manuell erfasst und einander zugeordnet werden.

Ausführliche Informationen zu den Grundlagen zur Behandlung und Administration von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Kontendefinitionen für Benutzerkonten auf Seite 25
- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 47
- Löschverzögerung für Benutzerkonten der kundendefinierten Zielsysteme festlegen auf Seite 60
- Benutzerkonten erstellen und bearbeiten auf Seite 116

Kontendefinitionen für Benutzerkonten

Um Benutzerkonten automatisch an Personen zu vergeben, kennt der One Identity Manager Kontendefinitionen. Kontendefinitionen können für jedes Zielsystem erzeugt werden. Hat eine Person noch kein Benutzerkonto in einem Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Person ein neues Benutzerkonto erzeugt.

Aus den Personenstammdaten resultieren die Daten für das Benutzerkonto im jeweiligen Zielsystem. Die Personen müssen ein zentrales Benutzerkonto besitzen. Über die primäre Zuordnung der Person zu einem Standort, einer Abteilung, einer Kostenstelle oder einer Geschäftsrolle und die Zuweisung der IT Betriebsdaten zu diesen Unternehmensstrukturen wird automatisch die Zuteilung der IT Betriebsdaten zum Benutzerkonto der Person geregelt. Die Verarbeitung erfolgt über Bildungsregeln. In der Standardinstallation sind vordefinierte Bildungsregeln zur Ermittlung der benötigten Daten für die Benutzerkonten enthalten. Bei Bedarf können Sie die Bildungsregeln kundenspezifisch anpassen.

Für eine Kontendefinition legen Sie Automatisierungsgrade für die Behandlung der Benutzerkonten fest. Der Automatisierungsgrad eines Benutzerkontos entscheidet über den Umfang der vererbten Eigenschaften der Person an das Benutzerkonto. So kann beispielsweise eine Person mehrere Benutzerkonten in einem Zielsystem besitzen:

- Standardbenutzerkonto, welches alle Eigenschaften über die Person erbt
- Administratives Benutzerkonto, das zwar mit der Person verbunden ist, aber keine Eigenschaften von der Person erben soll

Ausführliche Informationen zu den Grundlagen zu Kontendefinitionen, Automatisierungsgraden und zur Ermittlung der gültigen IT Betriebsdaten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- Erstellen von Kontendefinitionen
- Konfigurieren der Automatisierungsgrade

- Erstellen der Abbildungsvorschriften für die IT Betriebsdaten
- Erfassen der IT Betriebsdaten
- Zuweisen der Kontendefinitionen an Personen und Zielsysteme

Detaillierte Informationen zum Thema

- Kontendefinitionen erstellen auf Seite 26
- Kontendefinitionen bearbeiten auf Seite 27
- Stammdaten für Kontendefinitionen auf Seite 27
- Automatisierungsgrade bearbeiten auf Seite 30
- Automatisierungsgrade erstellen auf Seite 31
- Stammdaten für Automatisierungsgrade auf Seite 32
- Abbildungsvorschrift für IT Betriebsdaten erstellen auf Seite 33
- IT Betriebsdaten erfassen auf Seite 34
- IT Betriebsdaten ändern auf Seite 36
- Zuweisen der Kontendefinitionen an Personen auf Seite 37
- Kontendefinitionen an kundendefinierte Zielsysteme zuweisen auf Seite 44
- Kontendefinition löschen auf Seite 45

Kontendefinitionen erstellen

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten der Kontendefinition.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Stammdaten für Kontendefinitionen auf Seite 27
- Kontendefinitionen bearbeiten auf Seite 27
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 31

Kontendefinitionen bearbeiten

Um eine Kontendefinition zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Kontendefinition.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Kontendefinitionen auf Seite 27
- Kontendefinitionen erstellen auf Seite 26
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 31

Stammdaten für Kontendefinitionen

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 6: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Angabe der vorausgesetzten Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch zugeordnet.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Personen. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER |**

Eigenschaft	Beschreibung
	CalculateRiskIndex aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Gibt an, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.
Automatische Zuweisung zu Personen	Gibt an, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Um die Kontendefinition automatisch an alle internen Personen zuzuweisen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Personen aktivieren**. Die Kontendefinition wird an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine neue interne Person erstellt wird, erhält diese Person ebenfalls automatisch diese Kontendefinition. Um die automatische Zuweisung der Kontendefinition von allen Personen zu entfernen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Personen deaktivieren**. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.

Eigenschaft	Beschreibung
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei verzögertem Löschen beibehalten	Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei Sicherheitsgefährdung beibehalten	Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Ressourcentyp	Ressourcentyp zur Gruppierung von Kontendefinitionen.
Freies Feld 01- Freies Feld 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Systemberechtigungen 1 erbbar Systemberechtigungen 2 erbbar Systemberechtigungen 3 erbbar	Gibt an, ob das Benutzerkonto Systemberechtigungen des entsprechenden Typs über die verbundene Person erben darf. Ist die Option aktiviert, werden Systemberechtigungen über hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Systemberechtigungen zugewiesen haben, dann erbt das Benutzerkonto diese Systemberechtigungen. • Wenn eine Person eine Zuweisung zu einer Systemberechtigung im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Systemberechtigung nur, wenn die Option aktiviert ist.

Automatisierungsgrade bearbeiten

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

- **Unmanaged**: Benutzerkonten mit dem Automatisierungsgrad **Unmanaged** erhalten eine Verbindung zur Person, erben jedoch keine weiteren Eigenschaften. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Person werden initial einige der Personeneigenschaften übernommen. Werden die Personeneigenschaften zu einem späteren Zeitpunkt geändert, dann werden diese Änderungen nicht an das Benutzerkonto weitergereicht.
- **Full managed**: Benutzerkonten mit dem Automatisierungsgrad **Full managed** erben definierte Eigenschaften der zugeordneten Person. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Person werden initial die Personeneigenschaften übernommen. Werden die Personeneigenschaften zu einem späteren Zeitpunkt geändert, dann werden diese Änderungen an das Benutzerkonto weitergereicht.

HINWEIS: Die Automatisierungsgrade **Full managed** und **Unmanaged** werden in Bildungsregeln ausgewertet. Die mitgelieferten Bildungsregeln können Sie im Designer unternehmensspezifisch anpassen.

Abhängig von Ihren Anforderungen können Sie weitere Automatisierungsgrade definieren. Die Bildungsregeln müssen Sie um die Vorgehensweise für die zusätzlichen Automatisierungsgrade erweitern.

Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll. Ausführliche Informationen zu Automatisierungsgraden finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

- Um die Berechtigungen zu entziehen, wenn eine Person deaktiviert, gelöscht oder als sicherheitsgefährdend eingestuft wird, können die Benutzerkonten der Person gesperrt werden. Wird die Person zu einem späteren Zeitpunkt wieder aktiviert, werden ihre Benutzerkonten ebenfalls wieder freigeschaltet.
- Zusätzlich kann die Vererbung der Gruppenmitgliedschaften definiert werden. Die Unterbrechung der Vererbung kann beispielsweise gewünscht sein, wenn die Benutzerkonten einer Person gesperrt sind und somit auch nicht in Gruppen Mitglied sein dürfen. Während dieser Zeit sollen keine Vererbungsvorgänge für diese Personen berechnet werden. Bestehende Gruppenmitgliedschaften werden dann gelöscht!

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad.

3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Automatisierungsgrade auf Seite 32
- Automatisierungsgrade erstellen auf Seite 31
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 31

Automatisierungsgrade erstellen

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade **Unmanaged** und **Full managed**. Abhängig von Ihren Anforderungen können Sie weitere Automatisierungsgrade definieren.

WICHTIG: Erweitern Sie im Designer die Bildungsregeln um die Vorgehensweise für die zusätzlichen Automatisierungsgrade. Ausführliche Informationen zu Bildungsregeln finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um einen Automatisierungsgrad zu erstellen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Automatisierungsgrade**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten des Automatisierungsgrades.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Automatisierungsgrade auf Seite 32
- Automatisierungsgrade bearbeiten auf Seite 30
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 31

Automatisierungsgrade an Kontendefinitionen zuweisen

WICHTIG: Der Automatisierungsgrad **Unmanaged** wird beim Erstellen einer Kontendefinition automatisch zugewiesen und kann nicht entfernt werden.

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Automatisierungsgrade zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Automatisierungsgrade zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Automatisierungsgraden entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Automatisierungsgrad und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Stammdaten für Automatisierungsgrade

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 7: Stammdaten eines Automatisierungsgrades

Eigenschaft	Beschreibung
Automatisierungsgrad	Bezeichnung des Automatisierungsgrades.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Betriebsdaten überschreibend	Gibt an, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind: • **Niemals**: Die Daten werden nicht aktualisiert. (Standard) • **Immer**: Die Daten werden immer aktualisiert. • **Nur initial**: Die Daten werden nur initial ermittelt.
Gruppen bei zeitweiliger Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.

Eigenschaft	Beschreibung
Benutzerkonten bei dauerhafter Deaktivierung sperren	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.
Gruppen bei verzögertem Löschen beibehalten	Gibt an, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei verzögertem Löschen sperren	Gibt an, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Gibt an, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

Abbildungsvorschrift für IT Betriebsdaten erstellen

Eine Kontendefinition legt fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über die primären Rollen einer Person ermittelt werden können.

Die folgenden IT Betriebsdaten werden in der Standardkonfiguration des One Identity Manager für das automatische Erzeugen und Ändern von Benutzerkonten für eine Person im Zielsystem verwendet.

- Container (je Zielsystem)
- Gruppen erbbar
- Identität
- Privilegiertes Benutzerkonto

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.

3. Wählen Sie die Aufgabe **IT Betriebsdaten Abbildungsvorschrift bearbeiten.**
4. Klicken Sie **Hinzufügen** und erfassen Sie folgende Informationen.
    - **Spalte**: Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
    - **Quelle**: Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen:
        - Primäre Abteilung
        - Primärer Standort
        - Primäre Kostenstelle
        - Primäre Geschäftsrolle

          HINWEIS: Die Geschäftsrolle kann nur verwendet werden, wenn das Geschäftsrollenmodul vorhanden ist.
        - keine Angabe

          Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option **Immer Standardwert verwenden** setzen.
    - **Standardwert**: Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
    - **Immer Standardwert verwenden**: Gibt an, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.
    - **Benachrichtigung bei Verwendung des Standards**: Gibt an, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkontos mit Standardwerten** verwendet.

      Um die Mailvorlage zu ändern, passen Sie im Designer den Konfigurationsparameter **TargetSystem | UNS | Accounts | MailTemplateDefaultValues** an.
5. Speichern Sie die Änderungen.

Verwandte Themen

- IT Betriebsdaten erfassen auf Seite 34

IT Betriebsdaten erfassen

Um für eine Person Benutzerkonten mit dem Automatisierungsgrad **Full managed** zu erzeugen, müssen die benötigten IT Betriebsdaten ermittelt werden. Welche IT

Betriebsdaten für welches Zielsystem konkret verwendet werden sollen, wird an den Geschäftsrollen, Abteilungen, Kostenstellen oder Standorten definiert. Einer Person wird eine primäre Geschäftsrolle, eine primäre Abteilung, eine primäre Kostenstelle oder ein primärer Standort zugeordnet. Abhängig von dieser Zuordnung werden die gültigen IT Betriebsdaten ermittelt und für die Erstellung des Benutzerkontos verwendet. Können über die primären Rollen keine gültigen IT Betriebsdaten ermittelt werden, werden die Standardwerte verwendet.

Wenn in einem Zielsystem mehrere Kontendefinitionen für die Abbildung der Benutzerkonten verwendet werden, können Sie die IT Betriebsdaten auch direkt für eine konkrete Kontendefinition festlegen.

Beispiel:

In der Regel erhält jede Person der Abteilung A ein Standardbenutzerkonto in der Domäne A. Zusätzlich erhalten einige Personen der Abteilung A administrative Benutzerkonten in der Domäne A.

Erstellen Sie eine Kontendefinition A für die Standardbenutzerkonten der Domäne A und eine Kontendefinition B für die administrativen Benutzerkonten der Domäne A. In der Abbildungsvorschrift der IT Betriebsdaten für die Kontendefinitionen A und B legen Sie die Eigenschaft **Abteilung** zur Ermittlung der gültigen IT Betriebsdaten fest.

Für die Abteilung A legen Sie die wirksamen IT Betriebsdaten für die Domäne A fest. Diese IT Betriebsdaten werden für die Standardbenutzerkonten verwendet. Zusätzlich legen Sie für die Abteilung A die wirksamen IT Betriebsdaten für die Kontendefinition B fest. Diese IT Betriebsdaten werden für administrative Benutzerkonten verwendet.

Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager in der Kategorie **Organisationen** oder **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.
3. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.
    - **Wirksam für**: Legen Sie den Anwendungsbereich der IT Betriebsdaten fest. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.

Um den Anwendungsbereich festzulegen

a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.

b. Wählen Sie unter **Tabelle** die Tabelle, die das Zielsystem abbildet oder, für eine Kontendefinition, die Tabelle `TSBAccountDef`.

c. Wählen Sie unter **Wirksam für** das konkrete Zielsystem oder die konkrete Kontendefinition.

d. Klicken Sie **OK**.

- **Spalte**: Wählen Sie die Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.

  In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden.

- **Wert**: Erfassen Sie den konkreten Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Abbildungsvorschrift für IT Betriebsdaten erstellen auf Seite 33

IT Betriebsdaten ändern

Sobald sich die IT Betriebsdaten ändern, müssen Sie diese Änderungen für bestehende Benutzerkonten übernehmen. Dafür führen Sie die Bildungsregeln an den betroffenen Spalten erneut aus. Bevor Sie die Bildungsregeln ausführen, prüfen Sie, welche Auswirkungen eine Änderung der IT Betriebsdaten auf bestehende Benutzerkonten hat. Für jede betroffene Spalte an jedem betroffenen Benutzerkonto können Sie entscheiden, ob die Änderung in die One Identity Manager-Datenbank übernommen werden soll.

Voraussetzungen

- Die IT Betriebsdaten einer Abteilung, einer Kostenstelle, einer Geschäftsrolle oder eines Standorts wurden geändert.

  - ODER -

- Die Standardwerte in der IT Betriebsdaten Abbildungsvorschrift für eine Kontendefinition wurden geändert.

HINWEIS: Ändert sich die Zuordnung einer Person zu einer primären Abteilung, Kostenstelle, zu einer primären Geschäftsrolle oder zu einem primären Standort, werden die Bildungsregeln automatisch ausgeführt.

Um die Bildungsregeln auszuführen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Bildungsregeln ausführen**.

   Es wird eine Liste aller Benutzerkonten angezeigt, die über die gewählte Kontendefinition entstanden sind und deren Eigenschaften durch die Änderung der IT Betriebsdaten geändert werden. Es bedeuten:

   - **Alter Wert**: Wert der Objekteigenschaft vor der Änderung der IT Betriebsdaten.
   - **Neuer Wert**: Wert der Objekteigenschaft nach der Änderung der IT Betriebsdaten.
   - **Auswahl**: Gibt an, ob der neue Wert für das Benutzerkonto übernommen werden soll.
4. Markieren Sie in der Spalte **Auswahl** alle Objekteigenschaften, für die der neue Wert übernommen werden soll.
5. Klicken Sie **Übernehmen**.

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinitionen an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

Das Standardverfahren für die Zuweisung von Kontendefinitionen an Personen ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen. Die Personen werden gemäß ihrer Funktion im Unternehmen in diese Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet und erhalten so ihre Kontendefinitionen. Um auf Sonderanforderungen zu reagieren, können einzelne Kontendefinitionen direkt an Personen zugewiesen werden.

Kontendefinitionen können automatisch an alle Personen eines Unternehmens zugewiesen werden. Es ist möglich, die Kontendefinitionen als bestellbare Produkte dem IT Shop zuzuordnen. Der Abteilungsleiter kann dann für seine Mitarbeiter Benutzerkonten über das Web Portal bestellen. Zusätzlich ist es möglich, Kontendefinitionen in Systemrollen aufzunehmen. Diese Systemrollen können über hierarchische Rollen oder direkt an Personen zugewiesen werden oder als Produkte in den IT Shop aufgenommen werden.

In den Prozessen der One Identity Manager Standardinstallation wird zunächst überprüft, ob die Person bereits ein Benutzerkonto im Zielsystem der Kontendefinition besitzt. Ist kein Benutzerkonto vorhanden, so wird ein neues Benutzerkonto mit dem Standardautomatisierungsgrad der zugewiesenen Kontendefinition erzeugt.

HINWEIS: Ist bereits ein Benutzerkonto vorhanden und ist es deaktiviert, dann wird dieses Benutzerkonto entsperrt. Den Automatisierungsgrad des Benutzerkontos müssen Sie in diesem Fall nachträglich ändern.

HINWEIS: Solange eine Kontendefinition für eine Person wirksam ist, behält die Person ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht.

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

- Für die Rollenklasse (Abteilung, Kostenstelle, Standort oder Geschäftsrolle) ist die Zuweisung von Personen und Kontendefinitionen erlaubt.

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

   - ODER -

   Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
   - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
   - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
3. Speichern Sie die Änderungen.

Ausführliche Informationen zur Vorbereitung der Rollenklassen für die Zuweisung finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Detaillierte Informationen zum Thema

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 39
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 39
- Kontendefinitionen an alle Personen zuweisen auf Seite 40
- Kontendefinitionen direkt an Personen zuweisen auf Seite 41
- Kontendefinitionen an kundendefinierte Zielsysteme zuweisen auf Seite 44

Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

    TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Organisationen entfernen.

    Um eine Zuweisung zu entfernen

    - Wählen Sie die Organisation und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 39
- Kontendefinitionen an alle Personen zuweisen auf Seite 40
- Kontendefinitionen direkt an Personen zuweisen auf Seite 41

Kontendefinitionen an Geschäftsrollen zuweisen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Geschäftsrollen entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 39
- Kontendefinitionen an alle Personen zuweisen auf Seite 40
- Kontendefinitionen direkt an Personen zuweisen auf Seite 41

Kontendefinitionen an alle Personen zuweisen

Über diese Aufgaben wird die Kontendefinition an alle internen Personen zugewiesen. Personen, die als externe Personen gekennzeichnet sind, erhalten die Kontendefinition nicht. Sobald eine neue interne Person erstellt wird, erhält diese Person ebenfalls automatisch diese Kontendefinition. Die Zuweisung wird durch den DBQueue Prozessor berechnet.

WICHTIG: Führen Sie die Aufgabe nur aus, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen!

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Automatische Zuweisung zu Personen aktivieren**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Speichern Sie die Änderungen.

HINWEIS: Um die automatische Zuweisung der Kontendefinition von allen Personen zu entfernen, führen Sie die Aufgabe **Automatische Zuweisung zu Personen deaktivieren** aus. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen bleiben jedoch erhalten.

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 39

- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 39
- Kontendefinitionen direkt an Personen zuweisen auf Seite 41

Kontendefinitionen direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **An Personen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Personen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Person und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 39
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 39
- Kontendefinitionen an alle Personen zuweisen auf Seite 40

Kontendefinitionen an Systemrollen zuweisen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Systemrollenmodul vorhanden ist.

Kontendefinitionen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können Sie nur an Systemrollen zuweisen, bei denen diese Option ebenfalls aktiviert ist.

Um Kontendefinitionen in eine Systemrolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Kontendefinitionen in den IT Shop aufnehmen

Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann sie von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die Kontendefinition muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Kontendefinition muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Kontendefinition im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.

- Soll die Kontendefinition nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss sie zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Kontendefinitionen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Kontendefinition in den IT Shop aufzunehmen.

Um eine Kontendefinition in den IT Shop aufzunehmen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinition an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Kontendefinition in den IT Shop aufzunehmen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinition an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Kontendefinition aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Kontendefinition aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

5. Klicken Sie **OK**.

   Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Verwandte Themen

- Stammdaten für Kontendefinitionen auf Seite 27
- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 39
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 39
- Kontendefinitionen direkt an Personen zuweisen auf Seite 41
- Kontendefinitionen an Systemrollen zuweisen auf Seite 41

Kontendefinitionen an kundendefinierte Zielsysteme zuweisen

Wenn Sie die automatische Zuordnung von Benutzerkonten und Personen einsetzen und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen, sind folgende Voraussetzungen zu gewährleisten:

- Die Kontendefinition ist dem Zielsystem zugewiesen.
- Die Kontendefinition besitzt einen Standardautomatisierungsgrad.

Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **Kundendefinierte Zielsysteme** das Zielsystem.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.
4. Speichern Sie die Änderungen.

Für kundendefinierte Zielsysteme müssen Sie die automatische Zuordnung von Personen zu Benutzerkonten kundenspezifisch implementieren.

Detaillierte Informationen zum Thema

- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 47

Kontendefinition löschen

Sie können Kontendefinitionen löschen, wenn diese keinem Zielsystem, keiner Person, keiner hierarchischen Rolle und keiner anderen Kontendefinition als Vorgänger zugeordnet sind.

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Wählen Sie die Aufgabe **Automatische Zuweisung zu Personen deaktivieren**.
    e. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
    f. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **An Personen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.
    e. Speichern Sie die Änderungen.
3. Entfernen Sie die Zuordnung der Kontendefinition zu Abteilungen, Kostenstellen und Standorten.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Organisationen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Abteilungen, Kostenstellen und Standorte.
    e. Speichern Sie die Änderungen.

4. Entfernen Sie die Zuordnung der Kontendefinition zu Geschäftsrollen.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
    e. Speichern Sie die Änderungen.
5. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden.

    Ausführliche Informationen zum Abbestellen einer Bestellung finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.

    Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei rollenbasierter Anmeldung)

    a. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
    d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
    e. Klicken Sie **OK**.

        Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

    Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
    d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
    e. Klicken Sie **OK**.

        Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.
6. Entfernen Sie die Zuordnung der Kontendefinition als vorausgesetzte Kontendefinition einer anderen Kontendefinition. Solange die Kontendefinition Voraussetzung einer anderen Kontendefinition ist, kann sie nicht gelöscht werden.

Prüfen Sie alle Kontendefinitionen.

a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

d. Entfernen Sie in der Auswahlliste **Vorausgesetzte Kontendefinition** die Kontendefinition.

e. Speichern Sie die Änderungen.

7. Entfernen Sie die Zuordnung der Kontendefinition zum Zielsystem.

a. Wählen Sie im Manager in der Kategorie **Kundendefinierte Zielsysteme** das Zielsystem.

b. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

c. Entfernen Sie auf dem Tabreiter **Allgemein** die zugewiesenen Kontendefinitionen.

d. Speichern Sie die Änderungen.

8. Löschen Sie die Kontendefinition.

a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

c. Klicken Sie , um die Kontendefinition zu löschen.

Automatische Zuordnung von Personen zu Benutzerkonten

Beim Einfügen eines Benutzerkontos kann automatisch eine vorhandene Person zugeordnet werden. Im Bedarfsfall kann eine Person neu erstellt werden. Dabei werden die Personenstammdaten anhand vorhandener Benutzerstammdaten erzeugt. Dieser Mechanismus kann auf die Erstellung eines neuen Benutzerkontos durch manuelle Anlage oder Synchronisation folgen.

Für die automatische Personenzuordnung definieren Sie Kriterien für die Ermittlung der Personen. Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Person verbunden, so erhält das Benutzerkonto durch interne Verarbeitung den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

Schalten Sie das Verfahren im laufenden Betrieb ein, erfolgt ab diesem Zeitpunkt die automatische Zuordnung der Personen zu Benutzerkonten. Deaktivieren Sie das Verfahren zu einem späteren Zeitpunkt wieder, wirkt sich diese Änderung nur auf Benutzerkonten aus, die ab diesem Zeitpunkt angelegt oder aktualisiert werden. Bereits vorhandene Zuordnungen von Personen zu Benutzerkonten bleiben bestehen.

HINWEIS: Für administrative Benutzerkonten wird empfohlen, die Zuordnung der Personen nicht über die automatische Personenzuordnung vorzunehmen. Ordnen Sie Personen zu administrativen Benutzerkonten über die Aufgabe **Stammdaten bearbeiten** am jeweiligen Benutzerkonto zu.

Ausführliche Informationen zur automatischen Personenzuordnung finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Führen Sie folgende Aktionen aus, damit Personen automatisch zugeordnet werden können.

- Wenn Personen bei der Synchronisation von Benutzerkonten zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | UNS | PersonAutoFullsync** und wählen Sie den gewünschte Modus aus.
- Wenn Personen außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | UNS | PersonAutoDefault** und wählen Sie den gewünschten Modus aus.
- Legen Sie im Konfigurationsparameter **TargetSystem | UNS | PersonExcludeList** die Benutzerkonten fest, für die keine automatische Zuordnung zu Personen erfolgen soll.

  Beispiel:

  ```
  ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $
  ```

  TIPP: Den Wert des Konfigurationsparameters können Sie über den Dialog **Ausschlussliste für die automatische Personenzuordnung** bearbeiten.

  Um die Ausschlussliste für die automatische Personenzuordnung zu bearbeiten

  1. Bearbeiten Sie im Designer den Konfigurationsparameter **PersonExcludeList**.
  2. Klicken Sie **...** hinter dem Eingabefeld **Wert**.

     Der Dialog **Ausschlussliste für Benutzerkonten** wird geöffnet.
  3. Um einen neuen Eintrag einzufügen, klicken Sie **Neu**.

     Um einen Eintrag zu bearbeiten, wählen Sie den Eintrag und klicken Sie **Bearbeiten**.
  4. Erfassen Sie die Bezeichnung des Benutzerkontos, dem Personen nicht automatisch zugeordnet werden sollen.

     Jeder Eintrag in der Liste wird als Teil eines regulären Ausdrucks behandelt. Metazeichen für reguläre Ausdrücke können verwendet werden.

5. Um einen Eintrag zu löschen, wählen Sie den Eintrag und klicken Sie **Löschen**.
6. Klicken Sie **OK**.

- Legen Sie über den Konfigurationsparameter **TargetSystem | UNS | PersonAutoDisabledAccounts** fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
- Weisen Sie dem Zielsystem eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Personenzuordnung am Zielsystem.

  HINWEIS: Um die Herkunft der Personen zu bestimmen, können Sie im Skript `TSB_PersonAuto_Mapping_UNSAccountB` die Spalte `Person.ImportSource` bestücken. Erweitern Sie dazu im Designer die Liste der zulässigen Werte an der Spalte `Person.ImportSource` und überschreiben Sie das Skript entsprechend.

HINWEIS:

Für die Synchronisation gilt:

- Die automatische Personenzuordnung wirkt, wenn Benutzerkonten neu angelegt oder aktualisiert werden.

Außerhalb der Synchronisation gilt:

- Die automatische Personenzuordnung wirkt, wenn Benutzerkonten neu angelegt werden.

HINWEIS:

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für das Zielsystem bekannt, werden die Benutzerkonten mit den Personen verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand **Linked** (verbunden).

Um die Benutzerkonten über Kontendefinitionen zu verwalten, weisen Sie diesen Benutzerkonten eine Kontendefinition und einen Automatisierungsgrad zu.

Verwandte Themen

- Kontendefinitionen erstellen auf Seite 26
- Kontendefinitionen an kundendefinierte Zielsysteme zuweisen auf Seite 44
- Automatisierungsgrade für Benutzerkonten ändern auf Seite 52
- Kontendefinitionen an verbundene Benutzerkonten zuweisen auf Seite 53
- Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 50

Suchkriterien für die automatische Personenzuordnung bearbeiten

Die Kriterien für die Personenzuordnung werden an den Zielsystemen definiert. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person dem Benutzerkonto zugeordnet werden kann. Die Suchkriterien können Sie durch Formatdefinitionen weiter einschränken.

Das zusammengestellte Suchkriterium wird in XML-Notation in die Spalte **Suchkriterien für die automatische Personenzuordnung** (`AccountToPersonMatchingRule`) der Zielsystem-Tabelle geschrieben.

Die Suchkriterien werden bei der automatischen Zuordnung von Personen zu Benutzerkonten ausgewertet. Darüber hinaus können Sie anhand der Suchkriterien eine Vorschlagsliste für die Personenzuordnung an Benutzerkonten erzeugen und die Zuordnung direkt ausführen.

HINWEIS: Die Objektdefinitionen für Benutzerkonten, auf welche die Suchkriterien angewendet werden können, sind vordefiniert. Sollten Sie weitere Objektdefinitionen benötigen, um beispielsweise die Vorauswahl der Benutzerkonten weiter einzuschränken, erzeugen Sie im Designer die entsprechenden kundenspezifische Objektdefinitionen. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um Kriterien für die Personenzuordnung festzulegen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Zielsysteme**.
2. Wählen Sie in der Ergebnisliste das Zielsystem.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person mit dem Benutzerkonto verbunden wird.

   Tabelle 8: Standardsuchkriterien für Benutzerkonten

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
Benutzerkonten	Zentrales Benutzerkonto (CentralAccount)	Anmeldename (AccountName)

5. Speichern Sie die Änderungen.

Ausführliche Informationen zur Definition der Suchkriterien finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 47
- Personen suchen und direkt an Benutzerkonten zuordnen auf Seite 51

Personen suchen und direkt an Benutzerkonten zuordnen

Anhand der Suchkriterien können Sie eine Vorschlagsliste für die Personenzuordnung an Benutzerkonten erzeugen und die Zuordnung direkt ausführen. Die Benutzerkonten sind dafür in verschiedenen Ansichten zusammengestellt.

Tabelle 9: Ansichten zur manuellen Zuordnung

Ansicht	Beschreibung
Vorgeschlagene Zuordnungen	Die Ansicht listet alle Benutzerkonten auf, denen der One Identity Manager eine Person zuordnen kann. Dazu werden die Personen angezeigt, die durch die Suchkriterien ermittelt und zugeordnet werden können.
Zugeordnete Benutzerkonten	Die Ansicht listet alle Benutzerkonten auf, denen eine Person zugeordnet ist.
Ohne Personenzuordnung	Die Ansicht listet alle Benutzerkonten auf, denen keine Person zugeordnet ist und für die über die Suchkriterien keine passende Person ermittelt werden kann.

Um Suchkriterien auf die Benutzerkonten anzuwenden

TIPP: Mit Maus-Doppelklick auf einen Eintrag in den Ansichten werden das Benutzerkonto und die Person geöffnet und Sie können die Stammdaten einsehen.

Durch die Zuordnung von Personen an die Benutzerkonten entstehen verbundene Benutzerkonten (Zustand **Linked**). Um verwaltete Benutzerkonten zu erhalten (Zustand **Linked configured**), können Sie gleichzeitig eine Kontendefinition zuordnen.

Um Personen direkt über die Vorschlagsliste zuzuordnen

- Klicken Sie **Vorgeschlagene Zuordnungen**.
    1. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Person zugeordnet werden soll. Eine Mehrfachauswahl ist möglich.
    2. (Optional) Wählen Sie im Auswahlfeld **Diese Kontendefinition zuweisen** eine Kontendefinition und im Auswahlfeld **Diesen Automatisierungsgrad zuweisen** einen Automatisierungsgrad.
    3. Klicken Sie **Ausgewählte zuweisen.**

4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

- ODER -

- Klicken Sie **Ohne Personenzuordnung**.
  1. Klicken Sie **Person auswählen** für das Benutzerkonto, dem eine Person zugeordnet werden soll. Wählen Sie eine Person aus der Auswahlliste.
  2. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Personen zugeordnet werden sollen. Eine Mehrfachauswahl ist möglich.
  3. (Optional) Wählen Sie im Auswahlfeld **Diese Kontendefinition zuweisen** eine Kontendefinition und im Auswahlfeld **Diesen Automatisierungsgrad zuweisen** einen Automatisierungsgrad.
  4. Klicken Sie **Ausgewählte zuweisen**.
  5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

     Den ausgewählten Benutzerkonten werden die Personen zugeordnet, die in der Spalte **Person** angezeigt werden. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

Um Zuordnungen zu entfernen

- Klicken Sie **Zugeordnete Benutzerkonten**.
  1. Klicken Sie **Auswahl** für alle Benutzerkonten, deren Personenzuordnung entfernt werden soll. Mehrfachauswahl ist möglich.
  2. Klicken Sie **Ausgewählte entfernen**.
  3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

     Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

Automatisierungsgrade für Benutzerkonten ändern

Wenn Sie Benutzerkonten über die automatische Personenzuordnung erstellen, wird der Standardautomatisierungsgrad genutzt. Sie können den Automatisierungsgrad eines Benutzerkontos nachträglich ändern.

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.

3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Automatisierungsgrad** den Automatisierungsgrad.
5. Speichern Sie die Änderungen.

Kontendefinitionen an verbundene Benutzerkonten zuweisen

An Benutzerkonten im Zustand **Linked** (verbunden) kann nachträglich eine Kontendefinition zugewiesen werden. Das kann beispielsweise der Fall sein, wenn

- Personen und Benutzerkonten manuell verbunden wurden
- die automatische Personenzuordnung konfiguriert ist, beim Einfügen eines Benutzerkontos jedoch noch keine Kontendefinition an die Domäne zugeordnet ist

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten > Verbunden aber nicht konfiguriert > <Zielsystem>**.
    b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.
    c. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.
    d. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.
    e. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Kontendefinitionen an kundendefinierte Zielsysteme zuweisen auf Seite 44

Unterstützte Typen von Benutzerkonten

Im One Identity Manager können unterschiedliche Typen von Benutzerkonten wie beispielsweise Standardbenutzerkonten, administrative Benutzerkonten, Dienstkonten oder privilegierte Benutzerkonten abgebildet werden.

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identität

  Mit der Eigenschaft **Identität** (Spalte `IdentityType`) wird der Typ des Benutzerkontos beschrieben.

Tabelle 10: Identitäten von Benutzerkonten

Identität	Beschreibung	Wert der Spalte IdentityType
Primäre Identität	Standardbenutzerkonto einer Person.	Primary
Organisatorische Identität	Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.	Organizational
Persönliche Administratoridentität	Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird.	Admin
Zusatzidentität	Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken.	Sponsored
Gruppenidentität	Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird.	Shared
Dienstidentität	Dienstkonto.	Service

HINWEIS: Um mit Identitäten für Benutzerkonten zu arbeiten, benötigen die Personen ebenfalls Identitäten. Benutzerkonten, denen eine Identität zugeordnet ist, können Sie nur mit Personen verbinden, die dieselbe Identität haben.

Die primäre Identität, die organisatorische Identität und die persönliche Administratoridentität werden für die verschiedenen Benutzerkonten genutzt, mit denen ein und dieselbe Person ihre unterschiedlichen Aufgaben im Unternehmen ausführen kann.

Um Benutzerkonten mit einer persönlichen Administratoridentität oder einer organisatorischen Identität für eine Person bereitzustellen, richten Sie für die Person Subidentitäten ein. Diese Subidentitäten verbinden Sie mit den Benutzerkonten. Somit können für die unterschiedlichen Benutzerkonten die erforderlichen Berechtigungen erteilt werden.

Benutzerkonten mit einer Zusatzidentität, einer Gruppenidentität oder einer Dienstidentität verbinden Sie mit Pseudo-Personen, die keinen Bezug zu einer realen Person haben. Diese Pseudo-Personen werden benötigt, um Berechtigungen an die Benutzerkonten vererben zu können. Bei der Auswertung von Berichten,

Attestierungen oder Complianceprüfungen prüfen Sie, ob die Pseudo-Personen gesondert betrachtet werden müssen.

Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

- Privilegiertes Benutzerkonto

  Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) gekennzeichnet.

Detaillierte Informationen zum Thema

- Standardbenutzerkonten auf Seite 55
- Administrative Benutzerkonten auf Seite 56
- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 57
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 58
- Privilegierte Benutzerkonten auf Seite 59

Standardbenutzerkonten

In der Regel erhält jede Person ein Standardbenutzerkonto, das die Berechtigungen besitzt, die für die tägliche Arbeit benötigt werden. Die Benutzerkonten haben eine Verbindung zur Person. Über eine Kontendefinition und deren Automatisierungsgrade kann die Auswirkung der Verbindung und der Umfang der vererbten Eigenschaften der Person an die Benutzerkonten konfiguriert werden.

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

1. Erstellen Sie eine Kontendefinition und weisen Sie die Automatisierungsgrade **Unmanaged** und **Full managed** zu.
2. Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.
3. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

   Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

Welche IT Betriebsdaten erforderlich sind, ist abhängig vom Zielsystem. Für Standardbenutzerkonten werden folgende Einstellungen empfohlen:

- Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsGroupAccount` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert verwenden**.
- Verwenden Sie in der Abbildungsvorschrift für die Spalte `IdentityType` den Standardwert **Primary** und aktivieren Sie die Option **Immer Standardwert verwenden**.

4. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem. Wählen Sie unter **Wirksam für** das konkrete Zielsystem.

   Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.

5. Weisen Sie die Kontendefinition an die Personen zu.

   Durch die Zuweisung der Kontendefinition an eine Person wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

Verwandte Themen

- Kontendefinitionen für Benutzerkonten auf Seite 25

Administrative Benutzerkonten

Für bestimmte administrative Aufgaben, ist der Einsatz administrativer Benutzerkonten notwendig. Administrative Benutzerkonten werden in der Regel vom Zielsystem vorgegeben und haben feste Bezeichnungen und Anmeldenamen, wie beispielsweise **Administrator**.

Administrative Benutzerkonten werden durch die Synchronisation in den One Identity Manager eingelesen.

HINWEIS: Einige administrative Benutzerkonten können automatisch als privilegierte Benutzerkonten gekennzeichnet werden. Aktivieren Sie dazu im Designer den Zeitplan **Ausgewählte Benutzerkonten als privilegiert kennzeichnen**.

Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 57
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 58

Administrative Benutzerkonten für eine Person bereitstellen

Voraussetzungen

- Das Benutzerkonto muss als persönliche Administratoridentität gekennzeichnet sein.
- Die Person, die das Benutzerkonto nutzen soll, muss als persönliche Administratoridentität gekennzeichnet sein.
- Die Person, die das Benutzerkonto nutzen soll, muss mit einer Hauptidentität verbunden sein.

Um ein administratives Benutzerkonto für eine Person bereitzustellen

1. Kennzeichnen Sie das Benutzerkonto als persönliche Administratoridentität.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Persönliche Administratoridentität**.
2. Verbinden Sie das Benutzerkonto mit der Person, die dieses administrative Benutzerkonto nutzen soll.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Person, die dieses administrative Benutzerkonto nutzt.

    TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche eine neue Person erstellen.

Verwandte Themen

- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 58
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Administrative Benutzerkonten für mehrere Personen bereitstellen

Voraussetzung

- Das Benutzerkonto muss als Gruppenidentität gekennzeichnet sein.
- Es muss eine Pseudo-Person vorhanden sein. Die Pseudo-Person muss als Gruppenidentität gekennzeichnet sein und muss einen Manager besitzen.
- Die Personen, die das Benutzerkonto nutzen dürfen, müssen als primäre Identitäten gekennzeichnet sein.

Um ein administratives Benutzerkonto für mehrere Personen bereitzustellen

1. Kennzeichnen Sie das Benutzerkonto als Gruppenidentität.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Gruppenidentität**.
2. Verbinden Sie das Benutzerkonto mit einer Pseudo-Person.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Pseudo-Person.

    TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche eine neue Pseudo-Person erstellen.
3. Weisen Sie dem Benutzerkonto die Personen zu, die dieses administrative Benutzerkonto nutzen sollen.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Personen mit Nutzungsberechtigungen zuzuweisen**.
    d. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

    TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Personen entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie die Person und doppelklicken Sie  .

Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 57
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Privilegierte Benutzerkonten

Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) gekennzeichnet.

HINWEIS: Die Kriterien anhand derer Benutzerkonten automatisch als privilegiert erkannt werden, sind als Erweiterungen zur Sichtdefinition (ViewAddOn) an der Tabelle `TSBVAccountIsPrivDetectRule` (Tabelle vom Typ **Union**) definiert. Die Auswertung erfolgt im Skript `TSB_SetIsPrivilegedAccount`.

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

1. Erstellen Sie eine Kontendefinition. Erstellen Sie einen neuen Automatisierungsgrad für privilegierte Benutzerkonten und weisen Sie diesen Automatisierungsgrad an die Kontendefinition zu.
2. Wenn Sie verhindern möchten, dass die Eigenschaften für privilegierte Benutzerkonten überschrieben werden, setzen Sie für den Automatisierungsgrad die Eigenschaft **IT Betriebsdaten überschreibend** auf den Wert **Nur initial**. In diesem Fall werden die Eigenschaften einmalig beim Erstellen der Benutzerkonten befüllt.
3. Legen Sie für den Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.
4. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

   Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden, und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

   Welche IT Betriebsdaten erforderlich sind, ist abhängig vom Zielsystem. Für privilegierte Benutzerkonten werden folgende Einstellungen empfohlen:

   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsPrivilegedAccount` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert**

verwenden.

- Zusätzlich können Sie eine Abbildungsvorschrift für die Spalte `IdentityType` festlegen. Die Spalte besitzt verschiedene zulässige Werte, die privilegierte Benutzerkonten repräsentieren.
- Um zu verhindern, das privilegierte Benutzerkonten die Berechtigungen des Standardbenutzers erben, definieren Sie eine Abbildungsvorschrift für die Spalte `IsGroupAccount` mit dem Standardwert **0** und aktivieren Sie die Option **Immer Standardwert verwenden**.

5. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem.

   Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.

6. Weisen Sie die Kontendefinition direkt an die Personen zu, die mit privilegierten Benutzerkonten arbeiten sollen.

   Durch die Zuweisung der Kontendefinition an eine Person wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

TIPP: Wenn es unternehmensspezifisch erforderlich ist, dass die Anmeldenamen privilegierter Benutzerkonten einem definierten Namensschema folgen, legen Sie die Bildungsregel fest, nach der die Anmeldenamen gebildet werden.

Verwandte Themen

- Kontendefinitionen für Benutzerkonten auf Seite 25

Löschverzögerung für Benutzerkonten der kundendefinierten Zielsysteme festlegen

Über die Löschverzögerung legen Sie fest, wie lange die Benutzerkonten nach dem Auslösen des Löschens in der Datenbank verbleiben, bevor sie endgültig entfernt werden. Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Die Benutzerkonten werden zunächst deaktiviert oder gesperrt. Bis zum Ablauf der Löschverzögerung besteht die Möglichkeit die Benutzerkonten wieder zu aktivieren. Nach Ablauf der Löschverzögerung werden die Benutzerkonten aus der Datenbank gelöscht und ein Wiederherstellen ist nicht mehr möglich.

Sie haben die folgenden Möglichkeiten die Löschverzögerung zu konfigurieren.

- Globale Löschverzögerung: Die Löschverzögerung gilt für die Benutzerkonten in allen Zielsystemen. Der Standardwert ist **30** Tage.

  Erfassen Sie eine abweichende Löschverzögerung im Designer für die Tabelle `UNSAccountB` in der Eigenschaft **Löschverzögerungen [Tage]**.
- Zielsystemspezifische Löschverzögerung: Die Löschverzögerung kann je Zielsystem individuell konfiguriert werden. Diese Löschverzögerung überschreibt die globale Löschverzögerung.

  Um eine individuelle Löschverzögerung je Zielsystem zu ermöglichen

  1. Konfigurieren Sie im Manager die Löschverzögerungen für die Zielsysteme.
     a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Zielsysteme**.
     b. Wählen Sie in der Ergebnisliste ein Zielsystem und wählen Sie die Aufgabe **Stammdaten bearbeiten**.
     c. Auf dem Tabreiter **Allgemein** erfassen Sie unter **Löschverzögerung [Tage]** die Löschverzögerung für das Zielsystem in Tagen.
     d. Speichern Sie die Änderungen.
  2. Erstellen Sie im Designer für die Tabelle `UNSAccountB` ein **Skript (Löschverzögerung)**.

     Beispiel:

     Die Löschverzögerung der Benutzerkonten in einem kundendefinierten Zielsystem soll von der Löschverzögerung des Zielsystems (`UNSRootB.DeleteDelayDays`) abhängig sein. An der Tabelle `UNSAccountB` wird folgendes Skript eingetragen.

     ```
     If $FK(UID_UNSRootB).DeleteDelayDays:Int$ > 0 Then
          Value = $FK(UID_UNSRootB).DeleteDelayDays:Int$
     End If
     ```

- Objektspezifische Löschverzögerung: Die Löschverzögerung kann abhängig von bestimmten Eigenschaften der Benutzerkonten konfiguriert werden.

  Um eine objektspezifische Löschverzögerung zu nutzen, erstellen Sie im Designer für die Tabelle `UNSAccountB` ein **Skript (Löschverzögerung)**.

  Beispiel:

  Die Löschverzögerung für privilegierte Benutzerkonten soll 10 Tage betragen. An der Tabelle wird folgendes **Skript (Löschverzögerung)** eingetragen.

```
If $IsPrivilegedAccount:Bool$ Then
     Value = 10
End If
```

Ausführliche Informationen zum Bearbeiten der Tabellendefinitionen und zum Konfigurieren der Löschverzögerung im Designer finden Sie im *One Identity Manager Konfigurationshandbuch*.

Verwandte Themen

- Allgemeine Stammdaten für kundendefinierte Zielsysteme auf Seite 110
- Benutzerkonten löschen und wiederherstellen auf Seite 125

Managen der Zuweisungen von Gruppen und Systemberechtigungen

Gruppen und Systemberechtigungen bilden die Objekte ab, über die im Zielsystem der Zugriff auf die Zielsystemressourcen gesteuert wird. Ein Benutzerkonto erhält über seine Mitgliedschaften in den Gruppen oder Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Zielsystemressourcen.

Im One Identity Manager können Sie Gruppen und Systemberechtigungen direkt an die Benutzerkonten zuweisen oder über Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen vererben. Des Weiteren können Benutzer die Gruppen und Systemberechtigungen über das Web Portal bestellen. Dazu werden die Gruppen und Systemberechtigungen im IT Shop bereitgestellt.

Detaillierte Informationen zum Thema

Typen der verwendeten Systemberechtigungen festlegen

Viele Zielsysteme nutzen mehr als einen Gruppentyp, um die Berechtigungen abzubilden. Das können beispielsweise Gruppen, Rollen oder Berechtigungssets sein. Im One Identity Manager können vier verschiedene Typen abgebildet werden.

Tabelle 11: Typen der verwendeten Systemberechtigungen

Typ	Tabelle
Gruppen	UNSGroupB
Systemberechtigungen 1	UNSGroupB1
Systemberechtigungen 2	UNSGroupB2
Systemberechtigungen 3	UNSGroupB3

Beim Einrichten der Synchronisation entscheiden Sie, welche Typen in welchen Tabellen abgebildet werden.

Ein Benutzerkonto erhält über seine Zuweisungen zu den Gruppen oder Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Zielsystemressourcen. Abhängig vom Zielsystem werden die Zuweisungen entweder an den Benutzerkonten (benutzerbasierte Zuweisung) oder an den Gruppen oder Systemberechtigungen (berechtigungsbasierte Zuweisung) gepflegt. Im One Identity Manager können Sie das Verhalten entsprechend konfigurieren. Die Zuweisungen werden in den folgenden Tabellen gespeichert:

Tabelle 12: Benutzerbasierte Zuweisung

UNSAccountBHasUNSGroupB	**Gruppen: Zuweisungen zu Benutzerkonten**
UNSAccountBHasUNSGroupB1	**Systemberechtigungen 1: Zuweisungen zu Benutzerkonten**
UNSAccountBHasUNSGroupB2	**Systemberechtigungen 2: Zuweisungen zu Benutzerkonten**
UNSAccountBHasUNSGroupB3	**Systemberechtigungen 3: Zuweisungen zu Benutzerkonten**

Tabelle 13: Berechtigungsbasierte Zuweisung

UNSAccountBInUNSGroupB	**Benutzerkonten: Zuweisungen zu Gruppen**
UNSAccountBInUNSGroupB1	**Benutzerkonten: Zuweisungen zu Systemberechtigungen 1**
UNSAccountBInUNSGroupB2	**Benutzerkonten: Zuweisungen zu Systemberechtigungen 2**
UNSAccountBInUNSGroupB3	**Benutzerkonten: Zuweisungen zu Systemberechtigungen 3**

Um festzulegen, welche Typen von Systemberechtigungen genutzt werden

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Zielsysteme**.

2. Wählen Sie in der Ergebnisliste ein Zielsystem und wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Typen der verwendeten Systemberechtigungen** alle Typen, die im angebundenen Zielsystem genutzt werden.
4. Wählen Sie in der Auswahlliste **Benutzerkonto enthält Mitgliedschaften** alle Typen, für welche die Zuweisungen am Benutzerkonto gespeichert werden.
    a. Aktivieren Sie die Systemberechtigungen, für welche die Zuweisungen an den Benutzerkonten gespeichert werden.
    b. Deaktivieren Sie die Systemberechtigungen, für welche die Zuweisungen an den Systemberechtigungen gespeichert werden.
5. Speichern Sie die Änderungen.

Beispiel

In einem Zielsystem werden Berechtigungen als Gruppen und als Profile verwaltet. Zuweisungen zu Gruppen werden an den Gruppenobjekten gepflegt, Zuweisungen zu Profilen an den Benutzerkonten. Die Gruppen werden im One Identity Manager in der Tabelle `UNSGroupB` abgebildet, die Profile in der Tabelle `UNSGroupB1`.

- Aktivieren Sie in der Auswahlliste **Typen der verwendeten Systemberechtigungen** die Werte **Gruppe** und **Systemberechtigung 1**.
- Aktivieren Sie in der Auswahlliste **Benutzerkonto enthält Mitgliedschaften** nur den Wert **Systemberechtigung 1**.

Die Zuweisungen zu den Systemberechtigungen werden in den Tabellen `UNSAccountBHasUNSGroupB1` und `UNSAccountBInUNSGroupB` gespeichert.

HINWEIS: Wenn Sie Attestierungsverfahren, Complianceregeln oder Unternehmensrichtlinien über Systemberechtigungen einrichten, achten Sie darauf, die korrekten Zuweisungstabellen auszuwählen, um sowohl benutzerbasierte als auch berechtigungsbasierte Zuweisungen zu betrachten.

Um die Funktionen unabhängig von der Konfiguration der Zielsysteme einzurichten, nutzen Sie die Abbildung der Zielsysteme im Unified Namespace. In der Tabelle `UNSAccountInUNSGroup` sind sowohl benutzerbasierte als auch berechtigungsbasierte Zuweisungen für alle Typen von Systemberechtigungen abgebildet; die Tabelle `UNSGroup` enthält alle Systemberechtigungen unabhängig vom Typ.

Ausführliche Informationen zum Unified Namespace finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Ausführliche Informationen zur Attestierungsfunktion, zu Complianceregeln und Unternehmensrichtlinien finden Sie in folgenden Handbüchern:

One Identity Manager Administrationshandbuch für Attestierungen
One Identity Manager Administrationshandbuch für Complianceregeln
One Identity Manager Administrationshandbuch für Unternehmensrichtlinien

Verwandte Themen

- Allgemeine Stammdaten für kundendefinierte Zielsysteme auf Seite 110

Zuweisen von Gruppen und Systemberechtigungen an Benutzerkonten im One Identity Manager

Gruppen und Systemberechtigungen können einem Benutzerkonto direkt oder indirekt zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person sowie der Gruppen und Systemberechtigungen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein Benutzerkonto im Zielsystem, werden die Gruppen und Systemberechtigungen der Rollen an dieses Benutzerkonto vererbt. Sie können Gruppen und Systemberechtigungen an Benutzerkonten zuweisen, die zum selben Zielsystem oder zu unterschiedlichen Zielsystemen desselben Zielsystemtyps gehören. Weitere Informationen finden Sie unter Zielsystemtypen für kundendefinierte Zielsysteme auf Seite 149.

Des Weiteren können Gruppen und Systemberechtigungen im Web Portal bestellt werden. Dazu werden Personen als Kunden in einen Shop aufgenommen. Alle Gruppen und Systemberechtigungen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Gruppen und Systemberechtigungen werden nach erfolgreicher Genehmigung den Personen zugewiesen.

Über Systemrollen können Gruppen und Systemberechtigungen zusammengefasst und als Paket an Personen und Arbeitsplätze zugewiesen werden. Sie können Systemrollen erstellen, die ausschließlich Gruppen oder Systemberechtigungen enthalten. Ebenso können Sie in einer Systemrolle beliebige Unternehmensressourcen zusammenfassen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppen und Systemberechtigungen auch direkt an Benutzerkonten zuweisen.

Thema	Handbuch
Grundlagen zur Zuweisung von Unternehmensressourcen und zur Vererbung von Unternehmensressourcen	*One Identity Manager Administrationshandbuch für das Identity Management Basismodul* *One Identity Manager Administrationshandbuch für Geschäftsrollen*
Zuweisung von Unternehmensressourcen über IT Shop-Bestellungen	*One Identity Manager Administrationshandbuch für IT Shop*
Systemrollen	*One Identity Manager Administrationshandbuch für Systemrollen*

Detaillierte Informationen zum Thema

Voraussetzungen für indirekte Zuweisungen von Gruppen und Systemberechtigungen an Benutzerkonten

Bei der indirekten Zuweisung werden Personen, Gruppen und Systemberechtigungen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet. Für die indirekte Zuweisung von Gruppen und Systemberechtigungen prüfen Sie folgende Einstellungen und passen Sie die Einstellungen bei Bedarf an.

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen, Gruppen und Systemberechtigungen erlaubt.

   Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul.*

   Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

   1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

      - ODER -

      Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
    - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
    - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
3. Speichern Sie die Änderungen.

2. Einstellungen für die Zuweisung von Gruppen und Systemberechtigungen an Benutzerkonten.
    - Das Benutzerkonto ist mit einer Person verbunden.
    - Am Benutzerkonto sind die Optionen **Gruppen erbbar**, **Systemberechtigungen 1 erbbar**, **Systemberechtigungen 2 erbbar**, **Systemberechtigungen 3 erbbar** aktiviert.
    - Je nach Konfiguration des Zielsystemtyps, können Gruppen und Systemberechtigungen entweder nur an Benutzerkonten zugewiesen werden, die zum selben Zielsystem gehören, oder auch an Benutzerkonten, die zu unterschiedlichen Zielsystemen gehören. Weitere Informationen finden Sie unter Zielsystemtypen für kundendefinierte Zielsysteme auf Seite 149.

HINWEIS: Bei der Vererbung von Unternehmensressourcen über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen spielen unter Umständen weitere Konfigurationseinstellungen eine Rolle. So kann beispielsweise die Vererbung für eine Rolle blockiert sein oder die Vererbung an Personen nicht erlaubt sein. Ausführliche Informationen über die Grundlagen zur Zuweisung von Unternehmensressourcen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Benutzerkonten erstellen und bearbeiten auf Seite 116
- Stammdaten für Benutzerkonten auf Seite 117
- Gruppen in kundendefinierten Zielsystemen auf Seite 126
- Stammdaten für Gruppen auf Seite 127
- Systemberechtigungen in kundendefinierten Zielsystemen auf Seite 131
- Stammdaten für Systemberechtigungen auf Seite 132

Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Gruppe an Abteilungen, Kostenstellen oder Standorte zu, damit die Gruppe über diese Organisationen an Benutzerkonten vererbt wird.

Um eine Gruppe an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Organisationen entfernen.

   Um eine Zuweisung zu entfernen
   - Wählen Sie die Organisation und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Um Gruppen an eine Abteilung, eine Kostenstelle oder einen Standort zuzuweisen (bei nicht-rollenbasierter Anmeldung oder bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Organisationen > Abteilungen**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Organisationen > Kostenstellen**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Organisationen > Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe**Systemberechtigungen kundendefinierter Zielsysteme zuweisen**.
4. Wählen Sie den Tabreiter **Gruppen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Gruppen entfernen.

   Um eine Zuweisung zu entfernen
   - Wählen Sie die Gruppe und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Gruppen und Systemberechtigungen an Benutzerkonten auf Seite 67
- Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 70
- Gruppen an Geschäftsrollen zuweisen auf Seite 72
- Gruppen in Systemrollen aufnehmen auf Seite 74
- Gruppen in den IT Shop aufnehmen auf Seite 76
- Benutzerkonten direkt an eine Gruppe zuweisen auf Seite 81
- Gruppen direkt an ein Benutzerkonto zuweisen auf Seite 83

Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie eine Systemberechtigung an Abteilungen, Kostenstellen oder Standorte zu, damit die Systemberechtigung über diese Organisationen an Benutzerkonten vererbt wird.

Um eine Systemberechtigung an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Organisationen entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie die Organisation und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Um Systemberechtigungen an eine Abteilung, eine Kostenstelle oder einen Standort zuzuweisen (bei nicht-rollenbasierter Anmeldung oder bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Organisationen > Abteilungen**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Organisationen > Kostenstellen**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Organisationen > Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **Systemberechtigungen kundendefinierter Zielsysteme zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemberechtigungen zu.
   - Weisen Sie auf dem Tabreiter **Systemberechtigungen 1** die Systemberechtigungen 1 zu.
   - Weisen Sie auf dem Tabreiter **Systemberechtigungen 2** die Systemberechtigungen 2 zu.
   - Weisen Sie auf dem Tabreiter **Systemberechtigungen 3** die Systemberechtigungen 3 zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemberechtigungen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemberechtigung und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Gruppen und Systemberechtigungen an Benutzerkonten auf Seite 67
- Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 68
- Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 73
- Systemberechtigungen in Systemrollen aufnehmen auf Seite 75
- Systemberechtigungen in den IT Shop aufnehmen auf Seite 78
- Benutzerkonten direkt an eine Systemberechtigung zuweisen auf Seite 82
- Systemberechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 84

Gruppen an Geschäftsrollen zuweisen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

Weisen Sie die Gruppe an Geschäftsrollen zu, damit die Gruppe über diese Geschäftsrollen an Benutzerkonten vererbt wird.

Um eine Gruppe an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Geschäftsrollen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Um Gruppen an eine Geschäftsrolle zuzuweisen (bei nicht-rollenbasierter Anmeldung oder bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **Gruppen kundendefinierter Zielsysteme zuweisen**.
4. Wählen Sie den Tabreiter **Gruppen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Gruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Gruppen und Systemberechtigungen an Benutzerkonten auf Seite 67
- Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 73

- Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 68
- Gruppen in Systemrollen aufnehmen auf Seite 74
- Gruppen in den IT Shop aufnehmen auf Seite 76
- Benutzerkonten direkt an eine Gruppe zuweisen auf Seite 81
- Gruppen direkt an ein Benutzerkonto zuweisen auf Seite 83

Systemberechtigungen an Geschäftsrollen zuweisen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

Weisen Sie eine Systemberechtigung an Geschäftsrollen zu, damit die Systemberechtigung über diese Geschäftsrollen an Benutzerkonten vererbt wird.

Um eine Systemberechtigung an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Geschäftsrollen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Um Systemberechtigungen an eine Geschäftsrolle zuzuweisen (bei nicht-rollenbasierter Anmeldung oder bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.

3. Wählen Sie die Aufgabe **Systemberechtigungen kundendefinierter Zielsysteme zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemberechtigungen zu.
    - Weisen Sie auf dem Tabreiter **Systemberechtigungen 1** die Systemberechtigungen 1 zu.
    - Weisen Sie auf dem Tabreiter **Systemberechtigungen 2** die Systemberechtigungen 2 zu.
    - Weisen Sie auf dem Tabreiter **Systemberechtigungen 3** die Systemberechtigungen 3 zu.

    TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemberechtigungen entfernen.

    Um eine Zuweisung zu entfernen

    - Wählen Sie die Systemberechtigung und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Gruppen und Systemberechtigungen an Benutzerkonten auf Seite 67
- Gruppen an Geschäftsrollen zuweisen auf Seite 72
- Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 70
- Systemberechtigungen in Systemrollen aufnehmen auf Seite 75
- Systemberechtigungen in den IT Shop aufnehmen auf Seite 78
- Benutzerkonten direkt an eine Systemberechtigung zuweisen auf Seite 82
- Systemberechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 84

Gruppen in Systemrollen aufnehmen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Systemrollenmodul vorhanden ist.

Mit dieser Aufgabe nehmen Sie eine Gruppe in Systemrollen auf.

Wenn Sie eine Systemrolle an Personen zuweisen, wird die Gruppe an alle Benutzerkonten des kundendefinierten Zielsystems vererbt, die diese Personen besitzen.

HINWEIS: Gruppen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen*.

Um eine Gruppe an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Gruppen und Systemberechtigungen an Benutzerkonten auf Seite 67
- Systemberechtigungen in Systemrollen aufnehmen auf Seite 75
- Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 68
- Gruppen an Geschäftsrollen zuweisen auf Seite 72
- Gruppen in den IT Shop aufnehmen auf Seite 76
- Benutzerkonten direkt an eine Gruppe zuweisen auf Seite 81
- Gruppen direkt an ein Benutzerkonto zuweisen auf Seite 83

Systemberechtigungen in Systemrollen aufnehmen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Systemrollenmodul vorhanden ist.

Mit dieser Aufgabe nehmen Sie eine Systemberechtigung in Systemrollen auf.

Wenn Sie eine Systemrolle an Personen zuweisen, wird die Systemberechtigung an alle Benutzerkonten des kundendefinierten Zielsystems vererbt, die diese Personen besitzen.

HINWEIS: Systemberechtigungen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen*.

Um eine Systemberechtigung an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemrolle und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Gruppen und Systemberechtigungen an Benutzerkonten auf Seite 67
- Gruppen in Systemrollen aufnehmen auf Seite 74
- Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 70
- Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 73
- Systemberechtigungen in den IT Shop aufnehmen auf Seite 78
- Benutzerkonten direkt an eine Systemberechtigung zuweisen auf Seite 82
- Systemberechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 84

Gruppen in den IT Shop aufnehmen

Mit der Zuweisung einer Gruppe an ein IT Shop Regal kann sie von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die Gruppe muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Gruppe muss eine Leistungsposition zugeordnet sein.

TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Gruppe im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.

- Soll die Gruppe nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Gruppe zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen oder Benutzerkonten ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Gruppen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Gruppen in den IT Shop aufzunehmen.

Um eine Gruppe in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Gruppen kundendefinierter Zielsysteme** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppe an die IT Shop Regale zu.
6. Speichern Sie die Änderungen.

Um eine Gruppe aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Gruppen kundendefinierter Zielsysteme** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
6. Speichern Sie die Änderungen.

Um eine Gruppe aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen** (bei nicht-rollenbasierter Anmeldung).

- ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen > Gruppen kundendefinierter Zielsysteme** (bei rollenbasierter Anmeldung).

2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Gruppe wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Gruppe abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Gruppen und Systemberechtigungen an Benutzerkonten auf Seite 67
- Stammdaten für Gruppen auf Seite 127
- Systemberechtigungen in den IT Shop aufnehmen auf Seite 78
- Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 68
- Gruppen an Geschäftsrollen zuweisen auf Seite 72
- Gruppen in Systemrollen aufnehmen auf Seite 74
- Benutzerkonten direkt an eine Gruppe zuweisen auf Seite 81
- Gruppen direkt an ein Benutzerkonto zuweisen auf Seite 83

Systemberechtigungen in den IT Shop aufnehmen

Mit der Zuweisung einer Systemberechtigung an ein IT Shop Regal kann sie von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die Systemberechtigung muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Systemberechtigung muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Systemberechtigung im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.
- Soll die Systemberechtigung nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Systemberechtigung zusätzlich mit der Option

Verwendung nur im IT Shop gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen oder Benutzerkonten ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Systemberechtigungen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Systemberechtigungen in den IT Shop aufzunehmen.

Um eine Systemberechtigung in den IT Shop aufzunehmen

1. Bei nicht-rollenbasierter Anmeldung:

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.

   Bei rollenbasierter Anmeldung:

   Wählen Sie im Manager die Kategorie **Berechtigungen > Systemberechtigungen 1 kundendefinierter Zielsysteme**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Systemberechtigungen 2 kundendefinierter Zielsysteme**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Systemberechtigungen 3 kundendefinierter Zielsysteme**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemberechtigung an die IT Shop Regale zu.
6. Speichern Sie die Änderungen.

Um eine Systemberechtigung aus einzelnen Regalen des IT Shops zu entfernen

1. Bei nicht-rollenbasierter Anmeldung:

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

- ODER -

Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.

Bei rollenbasierter Anmeldung:

Wählen Sie im Manager die Kategorie **Berechtigungen > Systemberechtigungen 1 kundendefinierter Zielsysteme**.

- ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen > Systemberechtigungen 2 kundendefinierter Zielsysteme**.

- ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen > Systemberechtigungen 3 kundendefinierter Zielsysteme**.

2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Entfernen Sie im Bereich **Zuordnungen entfernen** die Systemberechtigung aus den IT Shop Regalen.
6. Speichern Sie die Änderungen.

Um eine Systemberechtigung aus allen Regalen des IT Shops zu entfernen

1. Bei nicht-rollenbasierter Anmeldung:

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.

   Bei rollenbasierter Anmeldung:

   Wählen Sie im Manager die Kategorie **Berechtigungen > Systemberechtigungen 1 kundendefinierter Zielsysteme**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Systemberechtigungen 2 kundendefinierter Zielsysteme**.

   - ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen > Systemberechtigungen 3 kundendefinierter Zielsysteme**.

2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Systemberechtigung wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Systemberechtigung abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Gruppen und Systemberechtigungen an Benutzerkonten auf Seite 67
- Stammdaten für Gruppen auf Seite 127
- Gruppen in den IT Shop aufnehmen auf Seite 76
- Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 70
- Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 73
- Systemberechtigungen in Systemrollen aufnehmen auf Seite 75
- Benutzerkonten direkt an eine Systemberechtigung zuweisen auf Seite 82
- Systemberechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 84

Benutzerkonten direkt an eine Gruppe zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppen direkt an Benutzerkonten zuweisen. Gruppen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um Benutzerkonten direkt an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Benutzerkonten entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie das Benutzerkonto und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Benutzerkonten direkt an eine Systemberechtigung zuweisen auf Seite 82
- Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 68
- Gruppen an Geschäftsrollen zuweisen auf Seite 72
- Gruppen in Systemrollen aufnehmen auf Seite 74
- Gruppen in den IT Shop aufnehmen auf Seite 76
- Gruppen direkt an ein Benutzerkonto zuweisen auf Seite 83
- Zielsystemtypen für kundendefinierte Zielsysteme auf Seite 149

Benutzerkonten direkt an eine Systemberechtigung zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Systemberechtigung direkt an Benutzerkonten zuweisen. Systemberechtigungen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um Benutzerkonten direkt an eine Systemberechtigung zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Benutzerkonten entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie das Benutzerkonto und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Benutzerkonten direkt an eine Gruppe zuweisen auf Seite 81
- Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 70
- Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 73
- Systemberechtigungen in Systemrollen aufnehmen auf Seite 75
- Systemberechtigungen in den IT Shop aufnehmen auf Seite 78
- Systemberechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 84
- Zielsystemtypen für kundendefinierte Zielsysteme auf Seite 149

Gruppen direkt an ein Benutzerkonto zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Gruppen direkt zuweisen. Gruppen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um Gruppen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Gruppen und Systemberechtigungen zuweisen**.
4. Wählen Sie den Tabreiter **Gruppen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Gruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie ✓.

6. Speichern Sie die Änderungen.

Verwandte Themen

- Systemberechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 84
- Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 68
- Gruppen an Geschäftsrollen zuweisen auf Seite 72
- Gruppen in Systemrollen aufnehmen auf Seite 74
- Gruppen in den IT Shop aufnehmen auf Seite 76
- Benutzerkonten direkt an eine Gruppe zuweisen auf Seite 81
- Zielsystemtypen für kundendefinierte Zielsysteme auf Seite 149

Systemberechtigungen direkt an ein Benutzerkonto zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Systemberechtigungen direkt zuweisen. Systemberechtigungen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um Systemberechtigungen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Gruppen und Systemberechtigungen zuweisen**.
4. Wählen Sie den Tabreiter **Systemberechtigungen 1**.

   - ODER -

   Wählen Sie den Tabreiter **Systemberechtigungen 2**.

   - ODER -

   Wählen Sie den Tabreiter **Systemberechtigungen 3**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemberechtigungen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemberechtigungen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemberechtigung und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Gruppen direkt an ein Benutzerkonto zuweisen auf Seite 83
- Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 70
- Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 73
- Systemberechtigungen in Systemrollen aufnehmen auf Seite 75
- Systemberechtigungen in den IT Shop aufnehmen auf Seite 78
- Benutzerkonten direkt an eine Systemberechtigung zuweisen auf Seite 82
- Zielsystemtypen für kundendefinierte Zielsysteme auf Seite 149

Wirksamkeit von Mitgliedschaften in Gruppen und Systemberechtigungen

HINWEIS: Die hier für Gruppen beschriebene Funktionalität gilt gleichermaßen für die Systemberechtigungen.

Bei der Zuweisung von Gruppen an Benutzerkonten kann es vorkommen, dass eine Person zwei oder mehr Gruppen erhält, die in dieser Kombination nicht auftreten dürfen. Um das zu verhindern, geben Sie die sich ausschließenden Gruppen bekannt. Dabei legen Sie für zwei Gruppen fest, welche der beiden Gruppen an Benutzerkonten wirksam werden soll, wenn beide zugewiesen sind.

Die Zuweisung einer ausgeschlossenen Gruppe ist jederzeit direkt, indirekt oder per IT Shop-Bestellung möglich. Anschließend ermittelt der One Identity Manager, ob diese Zuweisung wirksam ist.

HINWEIS:

- Ein wechselseitiger Ausschluss zweier Gruppen kann nicht definiert werden. Das heißt, die Festlegung "Gruppe A schließt Gruppe B aus" UND "Gruppe B schließt Gruppe A aus" ist nicht zulässig.
- Für eine Gruppe muss jede auszuschließende Gruppe einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.
- Ob die Mitgliedschaft einer ausgeschlossenen Gruppe in einer anderen Gruppe zulässig ist (Tabelle`UNSGroupBInUNSGroupB`), wird durch den One Identity Manager nicht überprüft.

Die Wirksamkeit der Zuweisungen wird in den Tabellen `UNSAccountBInUNSGroupB`/`UNSAccountBHasUNSGroupB` und `BaseTreeHasUNSGroupB` über die Spalte `XIsInEffect` abgebildet.

Beispiel: Wirksamkeit von Gruppenmitgliedschaften

- In einem Zielsystem ist eine Gruppe A mit Berechtigungen zum Auslösen von Bestellungen definiert. Eine Gruppe B berechtigt zum Anweisen von Zahlungen. Eine Gruppe C berechtigt zum Prüfen von Rechnungen.
- Gruppe A wird über die Abteilung "Marketing", Gruppe B über die Abteilung "Finanzen" und Gruppe C wird über die Geschäftsrolle "Kontrollgruppe" zugewiesen.

Clara Harris hat ein Benutzerkonto in diesem Zielsystem. Sie gehört primär der Abteilung "Marketing" an. Sekundär sind ihr die Geschäftsrolle "Kontrollgruppe" und die Abteilung "Finanzen" zugewiesen. Ohne Ausschlussdefinition erhält das Benutzerkonto alle Berechtigungen der Gruppen A, B und C.

Durch geeignete Maßnahmen soll verhindert werden, dass eine Person sowohl Bestellungen auslösen als auch Rechnungen zur Zahlung anweisen kann. Das heißt, die Gruppen A und B schließen sich aus. Eine Person, die Rechnungen prüft, darf ebenfalls keine Rechnungen zur Zahlung anweisen. Das heißt, die Gruppen B und C schließen sich aus.

Tabelle 14: Festlegen der ausgeschlossenen Gruppen (Tabelle `UNSGroupBExclusion`)

Wirksame Gruppe	Ausgeschlossene Gruppe
Gruppe A	
Gruppe B	Gruppe A
Gruppe C	Gruppe B

Tabelle 15: Wirksame Zuweisungen

Person	Mitglied in Rolle	Wirksame Gruppe
Ben King	Marketing	Gruppe A
Jan Bloggs	Marketing, Finanzen	Gruppe B
Clara Harris	Marketing, Finanzen, Kontrollgruppe	Gruppe C
Jenny Basset	Marketing, Kontrollgruppe	Gruppe A, Gruppe C

Für Clara Harris ist nur die Zuweisung der Gruppe C wirksam und wird ins Zielsystem publiziert. Verlässt Clara Harris die Geschäftsrolle "Kontrollgruppe" zu einem späteren Zeitpunkt, wird die Gruppe B ebenfalls wirksam.

Für Jenny Basset sind die Gruppen A und C wirksam, da zwischen beiden Gruppen kein Ausschluss definiert wurde. Das heißt, die Person ist berechtigt Bestellungen

auszulösen und Rechnungen zu prüfen. Soll das verhindert werden, definieren Sie einen weiteren Ausschluss für die Gruppe C.

Tabelle 16: Ausgeschlossene Gruppen und wirksame Zuweisungen

Person	Mitglied in Rolle	Zugewiesene Gruppe	Ausgeschlossene Gruppe	Wirksame Gruppe
Jenny Basset	Marketing	Gruppe A		Gruppe C
	Kontrollgruppe	Gruppe C	Gruppe B Gruppe A	

Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherite | GroupExclusion** ist aktiviert.

  Aktivieren Sie im Designer den Konfigurationsparameter und kompilieren Sie die Datenbank.

  HINWEIS: Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.

- Sich ausschließende Gruppen gehören zum selben Zielsystem oder zum selben Zielsystemtyp.

HINWEIS: Innerhalb eines Zielsystemtyps werden Gruppen, die sich gegenseitig ausschließen, unabhängig vom Zielsystem ermittelt. Diese Besonderheit muss bei der Ausschlussdefinition berücksichtigt werden.

Um Gruppen auszuschließen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste eine Gruppe.
3. Wählen Sie die Aufgabe **Gruppen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die sich mit der gewählten Gruppe ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Um Systemberechtigungen auszuschließen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste eine Systemberechtigung.
3. Passend zur gewählten Systemberechtigung, wählen Sie die Aufgabe **Systemberechtigungen 1 ausschließen**, **Systemberechtigungen 2 ausschließen** oder **Systemberechtigungen 3 ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemberechtigungen zu, die sich mit der gewählten Systemberechtigung ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Systemberechtigungen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Vererbung von Gruppen und Systemberechtigungen anhand von Kategorien

HINWEIS: Die hier für Gruppen beschriebene Funktionalität gilt gleichermaßen für die Systemberechtigungen.

Im One Identity Manager können Gruppen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In der Gruppentabelle geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 63**.

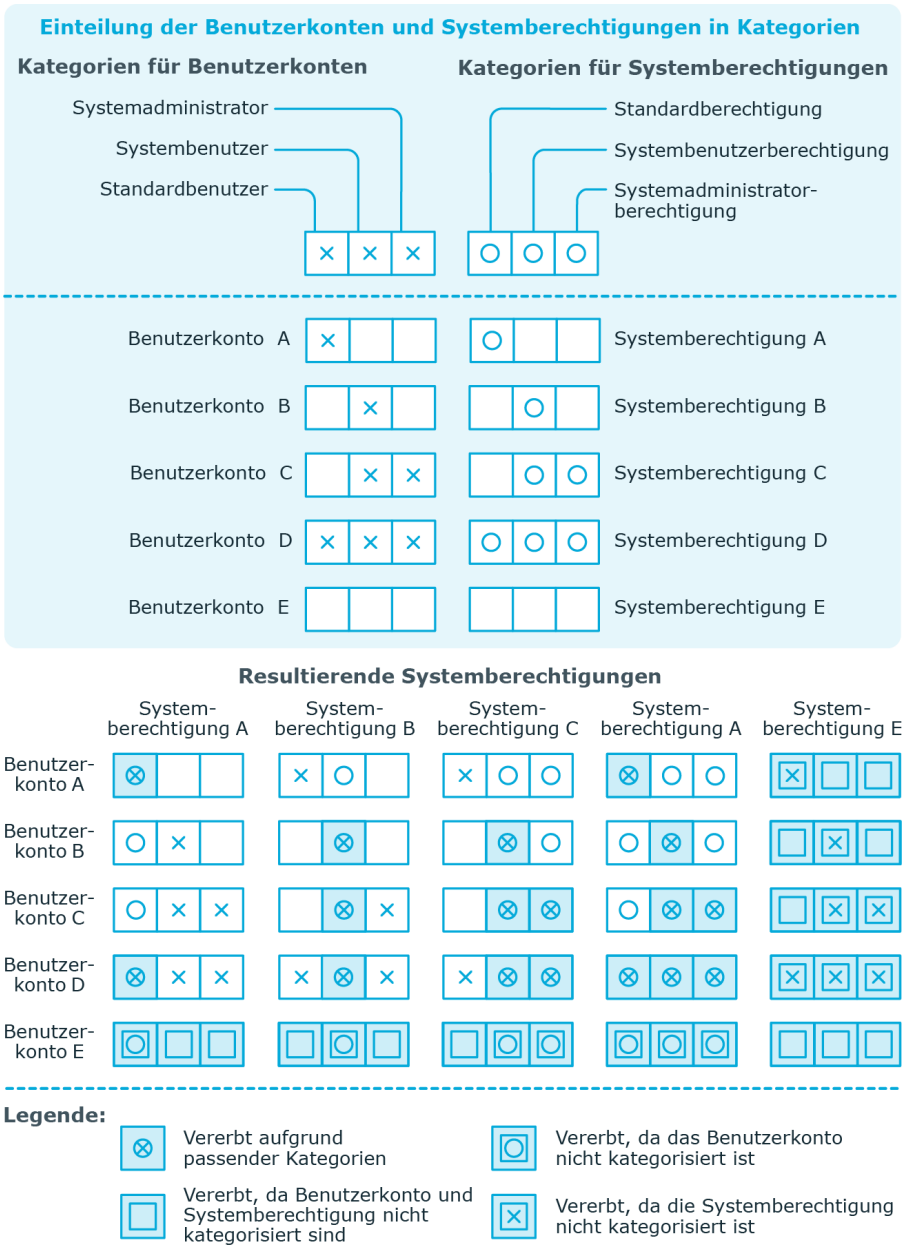
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist die Gruppe oder das Benutzerkonto nicht in Kategorien eingestuft, dann wird die Gruppe ebenfalls an das Benutzerkonto vererbt.

HINWEIS: Die Vererbung über Kategorien wird nur bei der indirekten Zuweisung von Gruppen über hierarchische Rollen berücksichtigt. Bei der direkten Zuweisung von Gruppen an Benutzerkonten werden die Kategorien nicht berücksichtigt.

Tabelle 17: Beispiele für Kategorien

Kategorieposition	Kategorien für Benutzerkonten	Kategorien für Gruppen
1	Standardbenutzer	Standardberechtigung
2	Systembenutzer	Systembenutzerberechtigung
3	Systemadministrator	Systemadministratorberechtigung

Abbildung 1: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

- Definieren Sie im Manager am Zielsystem die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Gruppen und Systemberechtigungen über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von Gruppen und Systemberechtigungen definieren auf Seite 113
- Stammdaten für Benutzerkonten auf Seite 117
- Stammdaten für Gruppen auf Seite 127
- Stammdaten für Systemberechtigungen auf Seite 132

Übersicht aller Zuweisungen

Für einige Objekte, wie beispielsweise Berechtigungen, Complianceregeln oder Rollen wird der Bericht **Übersicht aller Zuweisungen** angezeigt. Der Bericht ermittelt alle Rollen, wie beispielsweise Abteilungen, Kostenstellen, Standorte, Geschäftsrollen und IT Shop Strukturen, in denen sich Personen befinden, die das gewählte Basisobjekt besitzen. Dabei werden sowohl direkte als auch indirekte Zuweisungen des Basisobjektes berücksichtigt.

Beispiele:

- Wird der Bericht für eine Ressource erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Ressource besitzen.
- Wird der Bericht für eine Gruppe oder andere Systemberechtigung erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Gruppe oder Systemberechtigung besitzen.
- Wird der Bericht für eine Complianceregel erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Complianceregel verletzen.
- Wird der Bericht für eine Abteilung erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Abteilung ebenfalls Mitglied sind.
- Wird der Bericht für eine Geschäftsrolle erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Geschäftsrolle ebenfalls Mitglied sind.

Um detaillierte Informationen über Zuweisungen anzuzeigen

- Um den Bericht anzuzeigen, wählen Sie in der Navigation oder in der Ergebnisliste das Basisobjekt und wählen Sie den Bericht **Übersicht aller Zuweisungen**.
- Wählen Sie über die Schaltfläche **Verwendet von** in der Symbolleiste des Berichtes die Rollenklasse, für die Sie ermitteln möchten, ob es Rollen gibt, in denen sich Personen mit dem ausgewählten Basisobjekt befinden.

  Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des

Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.

- Mit einem Maus-Doppelklick auf das Steuerelement einer Rolle zeigen Sie alle untergeordneten Rollen der ausgewählten Rolle an.
- Mit einem einfachen Mausklick auf die Schaltfläche im Steuerelement einer Rolle zeigen Sie alle Personen dieser Rolle an, die das Basisobjekt besitzen.
- Über den Pfeil rechts neben der Schaltfläche starten Sie einen Assistenten, mit dem Sie die Liste der angezeigten Personen zur Nachverfolgung speichern können. Dabei wird eine neue Geschäftsrolle erstellt und die Personen werden der Geschäftsrolle zugeordnet.

Abbildung 2: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 18: Bedeutung der Symbole in der Symbolleiste des Berichts

Symbol	Bedeutung
	Anzeigen der Legende mit der Bedeutung der Steuerelemente des Berichts.
	Speichern der aktuellen Ansicht des Berichts als Bild.
	Auswählen der Rollenklasse, über die der Bericht erstellt werden soll.
	Anzeige aller Rollen oder Anzeige der betroffenen Rolle.

5

Bereitstellen von Anmeldeinformationen für Benutzerkonten

Wenn neue Benutzerkonten im One Identity Manager angelegt werden, werden sofort auch die zur Anmeldung am Zielsystem benötigten Kennwörter erstellt. Um das initiale Kennwort zu vergeben, stehen verschiedene Möglichkeiten zur Verfügung. Auf die Kennwörter werden vordefinierte Kennwortrichtlinien angewendet, die Sie bei Bedarf an Ihre Anforderungen anpassen können. Um die generierten Anmeldeinformationen an die Benutzer zu verteilen, können Sie E-Mail-Benachrichtigungen einrichten.

Detaillierte Informationen zum Thema

- Kennwortrichtlinien für Benutzerkonten auf Seite 93
- Initiales Kennwort für neue Benutzerkonten auf Seite 105
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 106

Kennwortrichtlinien für Benutzerkonten

Der One Identity Manager unterstützt Sie beim Erstellen von komplexen Kennwortrichtlinien beispielsweise für Systembenutzerkennwörter, das zentrale Kennwort von Personen sowie für Kennwörter für die einzelnen Zielsysteme. Kennwortrichtlinien werden sowohl bei der Eingabe eines Kennwortes durch den Anwender als auch bei der Generierung von Zufallskennwörtern angewendet.

In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können. Zusätzlich können Sie eigene Kennwortrichtlinien definieren.

Detaillierte Informationen zum Thema

- Vordefinierte Kennwortrichtlinien auf Seite 94
- Kennwortrichtlinien anwenden auf Seite 95

- Kennwortrichtlinien bearbeiten auf Seite 97
- Kennwortrichtlinien erstellen auf Seite 97
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 101
- Ausschlussliste für Kennwörter bearbeiten auf Seite 104
- Kennwörter prüfen auf Seite 104
- Generieren eines Kennwortes testen auf Seite 105
- Kennwortrichtlinien anwenden auf Seite 95

Vordefinierte Kennwortrichtlinien

Die vordefinierten Kennwortrichtlinien können Sie bei Bedarf an Ihre Anforderungen anpassen.

Kennwortrichtlinie für die Anmeldung am One Identity Manager

Für die Anmeldung am One Identity Manager wird die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** angewendet. Diese Kennwortrichtlinie definiert die Einstellung für die Kennwörter von Systembenutzern (`DialogUser.Password` und `Person.DialogUserPassword`) sowie für den Zugangscode für die einmalige Anmeldung am Web Portal (`Person.Passcode`).

HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

Ausführliche Informationen zu Kennwortrichtlinien für Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Personen

Bei entsprechender Konfiguration wird das zentrale Kennwort einer Person auf die Kennwörter der zielsystemspezifischen Benutzerkonten abgebildet. Die Kennwortrichtlinie **Kennwortrichtlinie für zentrales Kennwort von Personen** definiert die Einstellung für das zentrale Kennwort (`Person.CentralPassword`). Die Mitglieder der Anwendungsrolle **Identity Management | Personen | Administratoren** können diese Kennwortrichtlinie anpassen.

WICHTIG: Stellen Sie sicher, dass die Kennwortrichtlinie **Kennwortrichtlinie für zentrales Kennwort von Personen** nicht gegen die zielsystemspezifischen Anforderungen an Kennwörter verstößt.

Ausführliche Informationen zu Kennwortrichtlinien für Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Kennwortrichtlinien für Benutzerkonten

Es werden vordefinierte Kennwortrichtlinien bereitgestellt, die Sie auf die Kennwortspalten der Benutzerkonten anwenden können.

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie **One Identity Manager Kennwortrichtlinie**. Stellen Sie in diesem Fall sicher, dass die Standardrichtlinie nicht gegen die Anforderungen der Zielsysteme verstößt.

Für kundendefinierte Zielsysteme ist keine Kennwortrichtlinie vordefiniert. Erstellen Sie eigene Kennwortrichtlinien und wenden Sie diese auf die Benutzerkonten der kundendefinierten Zielsysteme (`UNSAccountB.UserPassword`).

Es wird empfohlen, für jedes kundendefinierte Zielsystem eine eigene Kennwortrichtlinie einzurichten. Sie können Kennwortrichtlinien auch auf Container-Ebene zuweisen.

Des Weiteren können Sie Kennwortrichtlinien abhängig von der Kontendefinition der Benutzerkonten oder abhängig vom Automatisierungsgrad der Benutzerkonten anwenden.

Kennwortrichtlinien anwenden

Für kundendefinierte Zielsysteme ist keine Kennwortrichtlinie vordefiniert. Erstellen Sie eigene Kennwortrichtlinien und wenden Sie diese auf die Benutzerkonten der kundendefinierten Zielsysteme (`UNSAccountB.UserPassword`).

Es wird empfohlen, für jedes kundendefinierte Zielsystem eine eigene Kennwortrichtlinie einzurichten. Sie können Kennwortrichtlinien auch auf Container-Ebene zuweisen.

Des Weiteren können Sie Kennwortrichtlinien abhängig von der Kontendefinition der Benutzerkonten oder abhängig vom Automatisierungsgrad der Benutzerkonten anwenden.

Die anzuwendende Kennwortrichtlinie für ein Benutzerkonto wird in folgender Reihenfolge ermittelt:

1. Kennwortrichtlinie der Kontendefinition des Benutzerkontos.
2. Kennwortrichtlinie des Automatisierungsgrades des Benutzerkontos.
3. Kennwortrichtlinie des Containers des Benutzerkontos.
4. Kennwortrichtlinie des Zielsystems des Benutzerkontos.
5. Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** (Standardrichtlinie).

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie **One Identity Manager Kennwortrichtlinie**. Stellen Sie in diesem Fall sicher, dass die Standardrichtlinie nicht gegen die Anforderungen der Zielsysteme verstößt.

Um eine Kennwortrichtlinie neu zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Klicken Sie im Bereich **Zuweisungen** die Schaltfläche **Hinzufügen** und erfassen Sie folgende Daten.
   - **Anwenden auf**: Anwendungsbereich der Kennwortrichtlinie.

     Um den Anwendungsbereich festzulegen

     1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.
     2. Wählen Sie unter **Tabelle** eine der folgenden Referenzen:
        - Die Tabelle, die die Basisobjekte der Synchronisation enthält.
        - Um die Kennwortrichtlinie abhängig von der Kontendefinition anzuwenden, wählen Sie die Tabelle **TSBAccountDef**.
        - Um die Kennwortrichtlinie abhängig vom Automatisierungsgrad anzuwenden, wählen Sie die Tabelle **TSBBehavoir**.
     3. Wählen Sie unter **Anwenden auf** die Tabelle, die die Basisobjekte enthält.
        - Wenn Sie die Tabelle mit den Basisobjekten der Synchronisation gewählt haben, dann wählen Sie das konkrete Zielsystem.
        - Wenn Sie die Tabelle **TSBAccountDef** gewählt haben, dann wählen Sie die konkrete Kontendefinition.
        - Wenn Sie die Tabelle **TSBBehavior** gewählt haben, dann wählen Sie den konkreten Automatisierungsgrad.
     4. Klicken Sie **OK**.
   - **Kennwortspalte**: Bezeichnung der Kennwortspalte.
   - **Kennwortrichtlinie**: Bezeichnung der Kennwortrichtlinie, die angewendet werden soll.
5. Speichern Sie die Änderungen.

Um die Zuweisung einer Kennwortrichtlinie zu ändern

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Wählen Sie im Bereich **Zuweisungen** die Zuweisung, die Sie ändern möchten.
5. Wählen Sie in der Auswahlliste **Kennwortrichtlinie** die neu anzuwendende Kennwortrichtlinie.
6. Speichern Sie die Änderungen.

Kennwortrichtlinien bearbeiten

In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können.

Um eine Kennwortrichtlinie zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Kennwortrichtlinie.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 98
- Richtlinieneinstellungen auf Seite 98
- Zeichenklassen für Kennwörter auf Seite 100
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 101

Kennwortrichtlinien erstellen

In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können. Zusätzlich können Sie eigene Kennwortrichtlinien definieren.

Um eine Kennwortrichtlinie zu erstellen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten der Kennwortrichtlinie.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 98
- Richtlinieneinstellungen auf Seite 98
- Zeichenklassen für Kennwörter auf Seite 100
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 101

Allgemeine Stammdaten für Kennwortrichtlinien

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 19: Stammdaten einer Kennwortrichtlinie

Eigenschaft	Bedeutung
Anzeigename	Bezeichnung der Kennwortrichtlinie. Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Fehlermeldung	Kundenspezifische Fehlermeldung, die ausgegeben wird, wenn die Richtlinie nicht erfüllt wird. Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Eigentümer (Anwendungsrolle)	Anwendungsrolle, deren Mitglieder die Kennwortrichtlinie konfigurieren können.
Standardrichtlinie	Kennzeichnung als Standardrichtlinie für Kennwörter. Die Option kann nicht geändert werden. HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

Richtlinieneinstellungen

Auf dem Tabreiter **Kennwort** definieren Sie folgende Einstellungen für eine Kennwortrichtlinie.

Tabelle 20: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wenn beim Erstellen eines Benutzerkontos kein Kennwort angegeben wird oder kein Zufallskennwort generiert wird, dann wird das initiale Kennwort benutzt.
Kennwortbestätigung	Kennwortwiederholung.
Min. Länge	Minimale Länge des Kennwortes. Geben Sie die Anzahl von

Eigenschaft	Bedeutung
	Zeichen an, die ein Kennwort haben muss. Ist der Wert **0**, ist kein Kennwort erforderlich.
Max. Länge	Maximale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben kann. Der maximal zulässige Wert ist **256**.
Max. Fehlanmeldungen	Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Die Anzahl der Fehlanmeldungen wird nur bei der Anmeldung am One Identity Manager berücksichtigt. Ist der Wert **0**, dann wird die Anzahl der Fehlanmeldungen nicht berücksichtigt. Die Angabe wird nur berücksichtigt, wenn die Anmeldung am One Identity Manager mit einem Systembenutzer- oder Personen-basierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen überschritten, kann sich die Person oder der Systembenutzer nicht mehr am One Identity Manager anmelden. Kennwörter gesperrter Personen und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.
Max. Tage gültig	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird. Ist der Wert **0**, dann läuft das Kennwort nicht ab.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert. Ist der Wert **0**, dann werden keine Kennwörter in der Kennwortchronik gespeichert.
Min. Kennwortstärke	Gibt an, wie sicher ein Kennwort sein muss. Je höher die Kennwortstärke, desto sicherer ist das Kennwort. Mit dem Wert **0** wird die Kennwortstärke nicht geprüft. Die Werte **1**, **2**, **3** und **4** geben die erforderliche Komplexität des Kennwortes an. Dabei stellt der Wert **1** die geringsten Anforderungen an die Komplexität eines Kennwortes. Der Wert **4** fordert die höchste Komplexität.
Namensbestandteile unzulässig	Gibt an, ob Namensbestandteile im Kennwort zulässig oder unzulässig sind. Ist die Option aktiviert, sind Namensbestandteile in Kennwörtern nicht zulässig. Es werden die Werte der Spalten berücksichtigt, für welche die Option **Enthält Namensbestandteile für die**

Eigenschaft	Bedeutung
	Kennwortprüfung aktiviert ist. Die Option passen Sie im Designer an der Spaltendefinition an. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Zeichenklassen für Kennwörter

Auf dem Tabreiter **Zeichenklassen** legen Sie fest, welche Zeichen für ein Kennwort zulässig sind.

Tabelle 21: Zeichenklassen für Kennwörter

Eigenschaft	Bedeutung
Erforderliche Anzahl von Zeichenklassen	Anzahl der Regeln für Zeichenklassen, die erfüllt sein müssen, damit ein Kennwort der Kennwortrichtlinie entspricht. Berücksichtigt werden die Regeln für **Min. Anzahl Buchstaben**, **Min. Anzahl Kleinbuchstaben**, **Min. Anzahl Großbuchstaben**, **Min. Anzahl Ziffern** und **Min. Anzahl Sonderzeichen**. Es bedeuten: • Wert **0**: Es müssen alle Zeichenklassenregeln erfüllt sein. • Wert **> 0**: Anzahl der Zeichenklassenregeln, die mindestens erfüllt sein müssen. Der Wert kann maximal der Anzahl der Regeln entsprechend, deren Wert **> 0** ist. HINWEIS: Die Prüfung erfolgt nicht für generierte Kennwörter.
Min. Anzahl Buchstaben	Gibt an, wie viele alphabetische Zeichen ein Kennwort mindestens enthalten muss.
Min. Anzahl Kleinbuchstaben	Gibt an, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Großbuchstaben	Gibt an, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Ziffern	Gibt an, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Gibt an, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss.
Zulässige Sonderzeichen	Liste zulässiger Sonderzeichen.
Max. identische Zeichen insgesamt	Maximale Anzahl identischer Zeichen, die insgesamt im Kennwort vorkommen dürfen.

Eigenschaft	Bedeutung
Max. identische Zeichen aufeinanderfolgend	Maximale Anzahl identischer Zeichen, die nacheinander wiederholt werden können.
Unzulässige Sonderzeichen	Liste unzulässiger Sonderzeichen.
Keine Klein-buchstaben erzeugen	Gibt an, ob ein generiertes Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keinen Großbuch-staben erzeugen	Gibt an, ob ein generiertes Kennwort Großbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Ziffern erzeugen	Gibt an, ob ein generiertes Kennwort Ziffern enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berück-sichtigt.
Keine Sonderzeichen erzeugen	Gibt an, ob ein generiertes Kennwort Sonderzeichen enthalten darf. Ist die Option aktiviert, sind nur Buchstaben, Zahlen und Leerzeichen in Kennwörtern erlaubt. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.

Kundenspezifische Skripte für Kennwortanforderungen

Kundenspezifische Skripte zum Prüfen und Generieren von Kennwörtern können Sie einsetzen, wenn die Anforderungen an Kennwörter mit den vorhandenen Einstellmöglichkeiten nicht abgebildet werden können. Skripte werden zusätzlich zu den anderen Einstellungen angewendet.

Detaillierte Informationen zum Thema

- Skript zum Prüfen eines Kennwortes auf Seite 101
- Skript zum Generieren eines Kennwortes auf Seite 103

Skript zum Prüfen eines Kennwortes

Ein Prüfskript können Sie einsetzen, wenn zusätzliche Richtlinien beim Prüfen eines Kennwortes angewendet werden sollen, die nicht mit den vorhandenen Einstellmöglichkeiten abgebildet werden können.

Syntax für Prüfskripte

```
Public Sub CCC_CustomPwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
```

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Kennwort, das zu prüfen ist

TIPP: Um das Basisobjekt zu verwenden, nutzen Sie die Eigenschaft `Entity` der `PasswordPolicy`-Klasse.

Beispiel: Skript zum Prüfen eines Kennwortes

Ein Kennwort in darf nicht mit **?** oder **!** beginnen. Das Kennwort darf nicht mit drei identischen Zeichen beginnen. Das Skript prüft ein gegebenes Kennwort auf Zulässigkeit.

```
Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or
            '!'")#)
        End If
    End If
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in
            password")#)
        End If
    End If
End Sub
```

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
    b. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.

c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

d. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Prüfskript** den Namen des Skriptes ein, das zum Prüfen eines Kennwortes verwendet wird.

e. Speichern Sie die Änderungen.

Verwandte Themen

- Skript zum Generieren eines Kennwortes auf Seite 103

Skript zum Generieren eines Kennwortes

Ein Generierungsskript können Sie einsetzen, wenn zusätzliche Richtlinien beim Generieren eines Zufallskennwortes angewendet werden sollen, die nicht mit den vorhandenen Einstellmöglichkeiten abgebildet werden können.

Syntax für Generierungsskripte

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
```

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Generiertes Kennwort

TIPP: Um das Basisobjekt zu verwenden, nutzen Sie die Eigenschaft `Entity` der `PasswordPolicy`-Klasse.

Beispiel: Skript zum Generieren eines Kennwortes

Das Skript ersetzt in Zufallskennwörtern die unzulässigen Zeichen **?** und **!** zu Beginn eines Kennwortes mit **_**.

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    ' replace invalid characters at first position
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            spwd.SetAt(0, CChar("_"))
        End If
    End If
```

```
End Sub
```

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
    b. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Generierungsskript** den Namen des Skriptes ein, das zum Generieren eines Kennwortes verwendet wird.
    e. Speichern Sie die Änderungen.

Verwandte Themen

- Skript zum Prüfen eines Kennwortes auf Seite 101

Ausschlussliste für Kennwörter bearbeiten

Um bestimmte Begriffe im Kennwort zu verbieten, nehmen Sie den Begriff in die Ausschlussliste auf.

HINWEIS: Die Ausschlussliste ist global für alle Kennwortrichtlinien gültig.

Um einen Begriff in die Ausschlussliste aufzunehmen

1. Wählen Sie im Designer die Kategorie **Basisdaten > Sicherheitseinstellungen > Kennwort Ausschlussliste**.
2. Erstellen Sie einen neuen Eintrag über den Menüeintrag **Objekt > Neu** und erfassen Sie den auszuschließenden Begriff.
3. Speichern Sie die Änderungen.

Kennwörter prüfen

Beim Prüfen eines Kennwortes werden alle definierten Einstellungen der Kennwortrichtlinie, kundenspezifische Skripte sowie die Ausschlussliste für Kennwörter berücksichtigt.

Um zu prüfen, ob ein Kennwort der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Test**.
5. Wählen Sie in der Auswahlliste **Basisobjekt für den Test** die Tabelle und das Objekt für die Prüfung.
6. Geben Sie im Eingabefeld **Kennwort überprüfen** das Kennwort ein.

   Neben dem Eingabefeld wird angezeigt, ob das Kennwort gültig ist.

Generieren eines Kennwortes testen

Beim Generieren eines Kennwortes werden alle definierten Einstellungen der Kennwortrichtlinie, kundenspezifische Skripte sowie die Ausschlussliste für Kennwörter berücksichtigt.

Um ein Kennwort zu generieren, das der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Test**.
5. Klicken Sie auf die Schaltfläche **Generieren**.

   Das generierte Kennwort wird angezeigt.

Initiales Kennwort für neue Benutzerkonten

Um das initiale Kennwort für neue Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung.

- Tragen Sie beim Erstellen des Benutzerkontos in den Stammdaten ein Kennwort ein.
- Vergeben Sie beim Erstellen von Benutzerkonten ein zufällig generiertes initiales Kennwort.
  - Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | UNS | Accounts | InitialRandomPassword**.

- Verwenden Sie zielsystemspezifische Kennwortrichtlinien und definieren Sie in den Kennwortrichtlinien die Zeichenklassen, die das Kennwort enthalten muss.
- Legen Sie fest, an welche Person das initiale Kennwort per E-Mail versendet wird.

Verwandte Themen

- Kennwortrichtlinien für Benutzerkonten auf Seite 93
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 106

E-Mail-Benachrichtigungen über Anmeldeinformationen

Die Anmeldeinformationen für neue Benutzerkonten können per E-Mail an eine festgelegte Person gesendet werden. Dabei werden zwei Benachrichtigungen versendet, die den Benutzernamen und das initiale Kennwort enthalten. Zur Erzeugung der Benachrichtigungen werden Mailvorlagen genutzt. In einer Mailvorlage sind die Mailtexte in verschiedenen Sprachen definiert. Somit wird bei Generierung einer E-Mail Benachrichtigung die Sprache des Empfängers berücksichtigt. In der Standardinstallation sind bereits Mailvorlagen enthalten, die Sie zur Konfiguration der Benachrichtigungsverfahren verwenden können.

Um Benachrichtigungen zu nutzen, sind folgende Voraussetzungen zu erfüllen:

1. Stellen Sie sicher, dass das E-Mail-Benachrichtungssystem im One Identity Manager konfiguriert ist. Ausführliche Informationen finden Sie im *One Identity Manager Installationshandbuch*.
2. Aktivieren Sie im Designer den Konfigurationsparameter **Common | MailNotification | DefaultSender** und geben Sie die Absenderadresse an, mit der die E-Mail Benachrichtigungen verschickt werden.
3. Stellen Sie sicher, dass alle Personen eine Standard-E-Mail-Adresse besitzen. An diese E-Mail Adresse werden die Benachrichtigungen versendet. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
4. Stellen Sie sicher, dass für alle Personen eine Sprachkultur ermittelt werden kann. Nur so erhalten die Personen die E-Mail Benachrichtigungen in ihrer Sprache. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Wenn bei der Neuanlage eines Benutzerkontos ein zufällig generiertes initiales Kennwort vergeben wird, werden die initialen Anmeldeinformationen für dieses Benutzerkonto per E-Mail an eine vorher festgelegt Person gesendet.

Um die initialen Anmeldeinformationen per E-Mail zu versenden

1. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | UNS | Accounts | InitialRandomPassword**.
2. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | UNS | Accounts | InitialRandomPassword | SendTo** und erfassen Sie als Wert den Empfänger der Benachrichtigung.
3. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | UNS | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName**.

   Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Person - Erstellung neues Benutzerkonto** versendet. Die Benachrichtigung enthält den Namen des Benutzerkontos.
4. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | UNS | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword**.

   Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** versendet. Die Benachrichtigung enthält das initiale Kennwort für das Benutzerkonto.

HINWEIS: Um andere als die Standardmailvorlagen für diese Benachrichtigungen zu nutzen, ändern Sie die Werte der Konfigurationsparameter.

Abbildung der Objekte für kundenspezifische Zielsysteme im One Identity Manager

Im One Identity Manager werden die Benutzerkonten, Gruppen, Systemberechtigungen, Containerstrukturen und zusätzliche Berechtigungselemente eines kundendefinierten Zielsystems abgebildet. Diese Objekte werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können im Manager angezeigt oder bearbeitet werden. Um die Objekte verschiedener kundendefinierter Zielsysteme in der One Identity Manager-Datenbank unterscheiden zu können, legen Sie für jedes Zielsystem eine Kennung fest.

Detaillierte Informationen zum Thema

- Kennungen für kundendefinierte Zielsysteme auf Seite 108
- Containerstrukturen in kundendefinierten Zielsystemen auf Seite 115
- Benutzerkonten in kundendefinierten Zielsystemen auf Seite 116
- Gruppen in kundendefinierten Zielsystemen auf Seite 126
- Systemberechtigungen in kundendefinierten Zielsystemen auf Seite 131
- Berichte über kundendefinierte Zielsysteme auf Seite 139

Kennungen für kundendefinierte Zielsysteme

Um die Objekte verschiedener kundendefinierter Zielsysteme in der One Identity Manager-Datenbank unterscheiden zu können, legen Sie für jedes Zielsystem eine Kennung fest. Jedes Objekt kann durch diese Kennung genau einem Zielsystem zugeordnet werden. Zu jeder Kennung können Sie weitere Eigenschaften erfassen, die das Zielsystem genauer beschreiben.

Um kundendefinierte Zielsysteme einzurichten

- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | UNS | CreateNewRoot** und kompilieren Sie die Datenbank.

  Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um Kennungen für Zielsysteme zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Zielsysteme**.
2. Wählen Sie in der Ergebnisliste ein Zielsystem aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Zielsystems.
4. Speichern Sie die Änderungen.

TIPP: Die Eigenschaften eines Zielsystems können Sie auch im Manager in der Kategorie **Kundendefinierte Zielsysteme > <Zielsystem>** bearbeiten.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für kundendefinierte Zielsysteme auf Seite 110
- Datensynchronisation für kundendefinierte Zielsysteme anpassen auf Seite 112
- Kategorien für die Vererbung von Gruppen und Systemberechtigungen definieren auf Seite 113
- Alternative Spaltenbezeichnungen festlegen auf Seite 114
- Löschverzögerung für Benutzerkonten der kundendefinierten Zielsysteme festlegen auf Seite 60

Allgemeine Stammdaten für kundendefinierte Zielsysteme

Für ein kundendefiniertes Zielsystem erfassen Sie die folgenden Stammdaten.

Tabelle 22: Stammdaten eines kundendefinierten Zielsystems

Eigenschaft	Beschreibung
Zielsystem	Kennung des Zielsystems.
Zielsystemtyp	Typ des Zielsystems. Über den Zielsystemtyp können mehrere kundendefinierte Zielsysteme zusammengefasst werden. Innerhalb eines Zielsystemtyps werden Benutzerkonten an Gruppen auch dann zugewiesen, wenn diese verschiedenen Zielsystemen angehören.
Kanonischer Name	Name des Zielsystems gemäß DNS Syntax an: `Name dieses Zielsystems.Name des übergeordneten Zielsystems.Name des Stammsystems`
Definierter Name	Definierter Name des Zielsystems. Der definierte Name wird zur Bildung der definierten Namen untergeordneter Objekte verwendet. Stellt das Zielsystem keinen definierten Namen bereit, können Sie hier beispielsweise die Bezeichnung des Zielsystems eintragen: Syntaxbeispiel: `DC = <Zielsystem>`
Anzeigename	Bezeichnung, unter der das Zielsystem in den Werkzeugen des One Identity Manager angezeigt wird.
Kontendefinition (initial)	Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für dieses Zielsystem die automatische Zuordnung von Personen zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet. Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.
Löschverzögerung [Tage]	Verzögerung der Ausführung von Löschoperationen in Tagen für dieses Zielsystem. Weitere Informationen finden Sie unter Löschverzögerung für Benutzerkonten der kundendefinierten Zielsysteme festlegen auf Seite 60.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen

Eigenschaft	Beschreibung
	festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte des Zielsystems, dem sie zugeordnet sind. Jedem Zielsystem können somit andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieses Zielsystems sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Synchronisiert durch	Art der Synchronisation, über welche die Daten zwischen dem Zielsystem und dem One Identity Manager synchronisiert werden. Sobald Objekte für dieses Zielsystem im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden. **Tabelle 23: Zulässige Werte** **Wert** / **Synchronisation durch** / **Provisionierung durch** Synchronisation per Skript / keine / Skript-Komponente des One Identity Manager Keine Synchronisation / keine / keine Wenn Sie **Synchronisation per Skript** festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen. Sie können Datenimporte mit dem Programm Data Import konfigurieren oder im Synchronization Editor eine Synchronisation mit dem CSV Konnektor einrichten.
Typen der verwendeten Systemberechtigungen	Typen von Systemberechtigungen, denen in diesem Zielsystem Benutzerkonten zugewiesen werden können.
Benutzerkonto enthält Mitgliedschaften	Gibt an, für welche Typen von Systemberechtigungen die Zuweisungen an den Benutzerkonten gepflegt werden. Aktivieren Sie die Typen, für welche die Zuweisungen an den Benutzerkonten gepflegt werden. Die Zuweisungen werden in den Tabellen `UNSAccountBHasUNSGroupB`, `UNSAccountBHasUNSGroupB1`, `UNSAccountBHasUNSGroupB2`, `UNSAccountBHasUNSGroupB3` gespeichert.

Eigenschaft	Beschreibung
	Deaktivieren Sie die Typen, für welche die Zuweisungen an den Systemberechtigungen gepflegt werden. Die Zuweisungen werden in den Tabellen UNSAccountBInUNSGroupB, UNSAccountBInUNSGroupB1, UNSAccountBInUNSGroupB2, UNSAccountBInUNSGroupB3 gespeichert. Beispiel: Im Eingabefeld **Typen der verwendeten Systemberechtigungen** sind die Werte **Gruppe** und **Systemberechtigung 1** ausgewählt. Im Eingabefeld **Benutzerkonto enthält Mitgliedschaften** ist nur der Wert **Systemberechtigung 1** ausgewählt. Die Zuweisungen zu Systemberechtigungen werden in den Tabellen UNSAccountBHasUNSGroupB1 (**Systemberechtigungen 1: Zuweisungen zu Benutzerkonten**) und UNSAccountBInUNSGroupB (**Benutzerkonten: Zuweisungen zu Gruppen**) gespeichert.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Gruppenmitgliedschaften als MVP	Gibt an, ob an Benutzerkonten dieses Zielsystems die Gruppenmitgliedschaften als Liste auf einer Multi-Valued-Property (MVP)-Spalte zusammengefasst werden (relevant für Datenimporte).
Containerstruktur	Gibt an, ob das Zielsystem eine Containerstruktur besitzt.

Verwandte Themen

- Zielsystemtypen für kundendefinierte Zielsysteme auf Seite 149
- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 47
- Zielsystemverantwortliche auf Seite 147
- Typen der verwendeten Systemberechtigungen festlegen auf Seite 63

Datensynchronisation für kundendefinierte Zielsysteme anpassen

Nehmen Sie spezielle Anpassungen für die Datensynchronisation zwischen der One Identity Manager-Datenbank und der Zielsystemumgebung vor. Für die Datensynchronisation werden die folgenden Informationen abgebildet.

Tabelle 24: Stammdaten für die Datensynchronisation

Eigenschaft	Beschreibung
Synchronisationsserver	Eindeutige Kennung des Servers. Wählen Sie aus der Auswahlliste den Server aus, der die Prozesse für das Zielsystem verarbeitet. Dieser Synchronisationsserver wird beispielsweise genutzt, wenn die Provisionierung über die Synchronisation per Skript erfolgt.
Keine Schreiboperationen	Mit dieser Option können Sie verhindern, dass Änderungen an Zielsystemobjekten aus der One Identity Manager-Datenbank in das Zielsystem provisioniert werden.

Verwandte Themen

- Jobserver für die Provisionierung der Daten in ein kundendefiniertes Zielsystem auf Seite 14

Kategorien für die Vererbung von Gruppen und Systemberechtigungen definieren

HINWEIS: Die hier für Gruppen beschriebene Funktionalität gilt gleichermaßen für die Systemberechtigungen.

Im One Identity Manager können Gruppen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In der Gruppentabelle geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 63**.

Voraussetzungen

- Stellen Sie sicher, dass die Tabellen `UNSAccountB`, `UNSGroupB` und `UNSRootB` an den Zielsystemtyp zugewiesen sind. Weitere Informationen finden Sie unter Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 20.

Um die Tabellen an den Zielsystemtyp zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp des kundendefinierten Zielsystems.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Tabellen `UNSAccountB`, `UNSGroupB` und `UNSRootB` zu.
    - Wenn verwendet, weisen Sie die Tabellen `UNSGroupB1`, `UNSGroupB2` und `UNSGroupB3` zu.
5. Speichern Sie die Änderungen.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **Kundendefinierte Zielsysteme** das Zielsystem.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wechseln Sie auf den Tabreiter **Abbildungsvorschrift Kategorien**.
4. Erweitern Sie den jeweiligen Basisknoten einer Tabelle.
5. Aktivieren Sie die Kategorie per Maus-Doppelklick auf das Symbol .
6. Tragen Sie eine beliebige Benennung der Kategorie für Benutzerkonten und Gruppen in der verwendeten Anmeldesprache ein.
7. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Vererbung von Gruppen und Systemberechtigungen anhand von Kategorien auf Seite 88

Alternative Spaltenbezeichnungen festlegen

Wenn auf den Stammdatenformularen abweichende Bezeichnungen der Eingabefelder benötigt werden, können Sie für jeden Objekttyp die alternativ zu verwendenden Spaltenbezeichnungen sprachabhängig festlegen.

Um alternative Spaltenbezeichnungen festzulegen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Zielsysteme**.
2. Wählen Sie in der Ergebnisliste ein Zielsystem und wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wechseln Sie auf den Tabreiter **Alternative Spaltenbezeichnungen**.
4. Öffnen Sie den Mitgliederbaum der Tabelle, deren Spaltenbezeichnungen angepasst werden sollen.

   Es werden alle Spalten dieser Tabelle mit den Standard-Spaltenbezeichnungen aufgelistet.
5. Tragen Sie eine beliebige Benennung in der verwendeten Anmeldesprache ein.
6. Speichern Sie die Änderungen.

Containerstrukturen in kundendefinierten Zielsystemen

Die Containerstruktur repräsentiert die Strukturelemente eines Zielsystems. Container werden in einer hierarchischen Baumstruktur dargestellt.

Um einen Container zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Containerstruktur**.
2. Wählen Sie in der Ergebnisliste den Container und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Containers.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Stammdaten für Container auf Seite 115

Stammdaten für Container

Zu einem Container erfassen Sie die folgenden Stammdaten.

Tabelle 25: Stammdaten eines Containers

Eigenschaft	Beschreibung
Zielsystem	Kennung des Zielsystems.
Bezeichnung	Name des Containers.
Kanonischer Name	Kanonischer Name des Containers. Der kanonische Name wird automatisch gebildet und sollte nicht geändert werden.
Definierter Name	Definierter Name des Containers. Der definierte Name wird per Bildungsregel ermittelt und sollte nicht geändert werden.
Objekt GUID	Unikale ID, unter der das Objekt im Zielsystem verwaltet wird.
Übergeordneter Container	Übergeordneter Container zur Abbildung einer hierarchischen Containerstruktur. Der definierte Name wird dann automatisch durch Bildungsregeln aktualisiert.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Benutzerkonten in kundendefinierten Zielsystemen

Die Benutzerkonten repräsentieren die Authentifizierungsobjekte eines Zielsystems. Ein Benutzerkonto erhält über seine Mitgliedschaften in Gruppen oder Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Zielsystemressourcen.

Ein Benutzerkonto kann im One Identity Manager mit einer Person verbunden sein. Ebenso können Sie die Benutzerkonten getrennt von Personen verwalten.

HINWEIS: Um Benutzerkonten für die Personen eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen. Einige der nachfolgend beschriebenen Stammdaten werden dabei über Bildungsregeln aus den Personenstammdaten gebildet.

HINWEIS: Sollen Personen ihre Benutzerkonten über Kontendefinitionen erhalten, müssen die Personen ein zentrales Benutzerkonto besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.

Verwandte Themen

- Managen von Benutzerkonten und Personen auf Seite 24
- Kontendefinitionen für Benutzerkonten auf Seite 25
- Managen der Zuweisungen von Gruppen und Systemberechtigungen auf Seite 63
- Benutzerkonten erstellen und bearbeiten auf Seite 116
- Stammdaten für Benutzerkonten auf Seite 117
- Zusatzeigenschaften an Benutzerkonten zuweisen auf Seite 122
- Berechtigungselemente an Benutzerkonten zuweisen auf Seite 123
- Benutzerkonten deaktivieren auf Seite 124
- Benutzerkonten löschen und wiederherstellen auf Seite 125
- Überblick über Benutzerkonten anzeigen auf Seite 126

Benutzerkonten erstellen und bearbeiten

Ein Benutzerkonto kann im One Identity Manager mit einer Person verbunden sein. Ebenso können Sie die Benutzerkonten getrennt von Personen verwalten.

HINWEIS: Um Benutzerkonten für die Personen eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen. Einige der nachfolgend beschriebenen Stammdaten werden dabei über Bildungsregeln aus den Personenstammdaten gebildet.

Um ein Benutzerkonto zu erstellen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

Um die Stammdaten eines Benutzerkontos zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Benutzerkontos.
5. Speichern Sie die Änderungen.

Um ein Benutzerkonto für eine Person manuell zuzuweisen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie ein Benutzerkonto zu.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Benutzerkonten auf Seite 117
- Managen von Benutzerkonten und Personen auf Seite 24
- Unterstützte Typen von Benutzerkonten auf Seite 53
- Kontendefinitionen für Benutzerkonten auf Seite 25

Stammdaten für Benutzerkonten

Zu einem Benutzerkonto erfassen Sie die folgenden Stammdaten.

Tabelle 26: Eigenschaften eines Benutzerkontos

Eigenschaft	Beschreibung
Person	Person, die das Benutzerkonto verwendet. Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Person bereits eingetragen. Wenn Sie das Benutzerkonto

Eigenschaft	Beschreibung
	manuell erstellen, können Sie die Person aus der Auswahlliste wählen. Für ein Benutzerkonto mit einer Identität vom Typ **Organisatorische Identität**, **Persönliche Administratoridentität**, **Zusatzidentität**, **Gruppenidentität** oder **Dienstidentität** können Sie eine neue Person erstellen. Klicken Sie dafür neben dem Eingabefeld und erfassen Sie die erforderlichen Personenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp.
Keine Verbindung mit einer Person erforderlich	Gibt an, ob dem Benutzerkonto absichtlich keine Person zugeordnet ist. Die Option wird automatisch aktiviert, wenn ein Benutzerkonto in der Ausschlussliste für die automatische Personenzuordnung enthalten ist oder eine entsprechende Attestierung erfolgt ist. Sie können die Option manuell setzen. Aktivieren Sie die Option, falls das Benutzerkonto mit keiner Person verbunden werden muss (beispielsweise, wenn mehrere Personen das Benutzerkonto verwenden). Wenn durch die Attestierung diese Benutzerkonten genehmigt werden, werden diese Benutzerkonten künftig nicht mehr zur Attestierung vorgelegt. Im Web Portal können Benutzerkonten, die nicht mit einer Person verbunden sind, nach verschiedenen Kriterien gefiltert werden.
Nicht mit einer Person verbunden	Zeigt an, warum für das Benutzerkonto die Option **Keine Verbindung mit einer Person erforderlich** aktiviert ist. Mögliche Werte sind: • **durch Administrator**: Die Option wurde manuell durch den Administrator aktiviert. • **durch Attestierung**: Das Benutzerkonto wurde attestiert. • **durch Ausschlusskriterium**: Das Benutzerkonto wird aufgrund eines Ausschlusskriteriums nicht mit einer Person verbunden. Das Benutzerkonto ist beispielsweise in der Ausschlussliste für die automatische Personenzuordnung enthalten (Konfigurationsparameter **PersonExcludeList**).
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der

Eigenschaft	Beschreibung
	zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden. HINWEIS: Über die Aufgabe **Entferne Kontendefinition** am Benutzerkonto können Sie das Benutzerkonto wieder in den Zustand **Linked** zurücksetzen. Dabei wird die Kontendefinition vom Benutzerkonto und von der Person entfernt. Das Benutzerkonto bleibt über diese Aufgabe erhalten, wird aber nicht mehr über die Kontendefinition verwaltet. Die Aufgabe entfernt nur Kontendefinitionen, die direkt zugewiesen sind (`XOrigin=1`).
Automatisierungsgrad	Automatisierungsgrad des Benutzerkontos. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten.
Zielsystem	Kennung des Zielsystems.
Vorname	Vorname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Nachname	Nachname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Container	Container in dem das Benutzerkonto erzeugt werden soll. Haben Sie eine Kontendefinition zugeordnet, wird der Container, abhängig vom Automatisierungsgrad, aus den gültigen IT Betriebsdaten der zugeordneten Person ermittelt. Bei der Auswahl des Containers wird per Bildungsregel der definierte Name für das Benutzerkonto ermittelt.
Anmeldename	Name, mit dem sich der Benutzer am Zielsystem anmeldet. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Bezeichnung	Bezeichnung des Benutzerkontos. Die Bezeichnung wird aus dem Vornamen und dem Nachnamen des Benutzers gebildet.
Kanonischer Name	Kanonischer Name des Benutzerkontos. Der kanonische Name wird automatisch gebildet und sollte nicht geändert werden.

Eigenschaft	Beschreibung
Definierter Name	Definierter Name des Benutzerkontos. Der definierte Name wird per Bildungsregel ermittelt und sollte nicht geändert werden.
Objekt GUID	Unikale ID, unter der das Objekt im Zielsystem verwaltet wird.
Anzeigename	Anzeigename des Benutzerkontos.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen an das Benutzerkonto. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Kontoverfallsdatum	Tag, bis zu welchem sich der Benutzer mit dem Benutzerkonto am Zielsystem anmelden kann. Wenn für eine Person ein Austrittsdatum festgelegt ist, wird, abhängig vom Automatisierungsgrad des Benutzerkontos, dieses Austrittsdatum als Kontoverfallsdatum übernommen. Ein bereits eingetragenes Kontoverfallsdatum des Benutzerkontos wird dabei überschrieben. HINWEIS: Wenn zu einem späteren Zeitpunkt das Austrittsdatum der Person gelöscht wird, bleibt das Kontoverfallsdatum des Benutzerkontos erhalten!
Letzte Anmeldung	Datum der letzten Anmeldung am Zielsystem.
Kennwort	Kennwort für das Benutzerkonto. Das zentrale Kennwort der zugeordneten Person kann auf das Kennwort des Benutzerkontos abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*. Wenn Sie ein zufällig generiertes initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen. Das Kennwort wird nach dem Publizieren in das Zielsystem aus der Datenbank gelöscht. HINWEIS: Beim Prüfen eines Benutzerkennwortes werden

Eigenschaft	Beschreibung
	die One Identity Manager Kennwortrichtlinien beachtet. Stellen Sie sicher, dass die Kennwortrichtlinie nicht gegen die Anforderungen des Zielsystems verstößt.
Kennwortbestätigung	Kennwortwiederholung.
Letzte Kennwortänderung	Datum der letzten Kennwortänderung.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Identität	Typ der Identität des Benutzerkontos. Zulässige Werte sind: • **Primäre Identität**: Standardbenutzerkonto einer Person. • **Organisatorische Identität**: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • **Persönliche Administratoridentität**: Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird. • **Zusatzidentität**: Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken. • **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.
Privilegiertes Benutzerkonto	Gibt an, ob es sich um ein privilegiertes Benutzerkonto handelt.
Gruppen erbbar	Gibt an, ob das Benutzerkonto Gruppen über die verbundene Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist.

Eigenschaft	Beschreibung
Systemberechtigungen 1 erbbar Systemberechtigungen 2 erbbar Systemberechtigungen 3 erbbar	Gibt an, ob das Benutzerkonto Systemberechtigungen des entsprechenden Typs über die verbundene Person erben darf. Ist die Option aktiviert, werden Systemberechtigungen über hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Systemberechtigungen zugewiesen haben, dann erbt das Benutzerkonto diese Systemberechtigungen. • Wenn eine Person eine Zuweisung zu einer Systemberechtigung im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Systemberechtigung nur, wenn die Option aktiviert ist.
Benutzerkonto ist deaktiviert	Gibt an, ob das Benutzerkonto gesperrt ist. Wird ein Benutzerkonto vorübergehend nicht benötigt, können Sie das Benutzerkonto über die Option zeitweilig deaktivieren.

Verwandte Themen

- Kontendefinitionen für Benutzerkonten auf Seite 25
- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 47
- Kennwortrichtlinien für Benutzerkonten auf Seite 93
- Initiales Kennwort für neue Benutzerkonten auf Seite 105
- Unterstützte Typen von Benutzerkonten auf Seite 53
- Vererbung von Gruppen und Systemberechtigungen anhand von Kategorien auf Seite 88
- Voraussetzungen für indirekte Zuweisungen von Gruppen und Systemberechtigungen an Benutzerkonten auf Seite 67
- Benutzerkonten deaktivieren auf Seite 124
- Allgemeine Stammdaten für kundendefinierte Zielsysteme auf Seite 110

Zusatzeigenschaften an Benutzerkonten zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Ausführliche Informationen zum Verwenden von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Zusatzeigenschaften entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Zusatzeigenschaft und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Berechtigungselemente an Benutzerkonten zuweisen

Mit dieser Aufgabe können Sie mehrere Berechtigungselemente an ein Benutzerkonto zuweisen.

Um Berechtigungselemente an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Berechtigungselemente zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungselemente zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Berechtigungselementen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Berechtigungselement und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Benutzerkonten an Berechtigungselemente zuweisen auf Seite 138

Benutzerkonten deaktivieren

Wie Sie Benutzerkonten deaktivieren, ist abhängig von der Art der Verwaltung der Benutzerkonten.

Szenario:

Die Benutzerkonten sind mit Personen verbunden und werden über Kontendefinitionen verwaltet.

Benutzerkonten, die über Kontendefinitionen verwaltet werden, werden deaktiviert, wenn die Person dauerhaft oder zeitweilig deaktiviert wird. Das Verhalten ist abhängig vom Automatisierungsgrad des Benutzerkontos. Benutzerkonten mit dem Automatisierungsgrad **Full managed** werden entsprechend der Einstellungen an der Kontendefinition deaktiviert. Für Benutzerkonten mit einem anderen Automatisierungsgrad konfigurieren Sie das gewünschte Verhalten an der Bildungsregel der Spalte `UNSAccountB.AccountDisabled`.

Szenario:

Die Benutzerkonten sind mit Personen verbunden. Es sind keine Kontendefinitionen zugeordnet.

Benutzerkonten, die mit Personen verbunden sind, jedoch nicht über Kontendefinitionen verwaltet werden, werden deaktiviert, wenn die Person dauerhaft oder zeitweilig deaktiviert wird. Das Verhalten ist abhängig vom Konfigurationsparameter **QER | Person | TemporaryDeactivation**.

- Ist der Konfigurationsparameter aktiviert, werden die Benutzerkonten einer Person deaktiviert, wenn die Person zeitweilig oder dauerhaft deaktiviert wird.
- Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der Person keinen Einfluss auf die verbundenen Benutzerkonten.

Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Benutzerkonto ist deaktiviert**.
5. Speichern Sie die Änderungen.

Szenario:

Benutzerkonten sind nicht mit Personen verbunden.

Um ein Benutzerkonto zu deaktivieren, das nicht mit einer Person verbunden ist

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Benutzerkonto ist deaktiviert**.
5. Speichern Sie die Änderungen.

Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.*

Verwandte Themen

- Benutzerkonten löschen und wiederherstellen auf Seite 125
- Kontendefinitionen erstellen auf Seite 26
- Automatisierungsgrade erstellen auf Seite 31

Benutzerkonten löschen und wiederherstellen

HINWEIS: Solange eine Kontendefinition für eine Person wirksam ist, behält die Person ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht.

Ein Benutzerkonto, das nicht über eine Kontendefinition entstanden ist, löschen Sie über die Ergebnisliste oder über die Menüleiste. Nach Bestätigung der Sicherheitsabfrage wird das Benutzerkonto im One Identity Manager zunächst zum Löschen markiert. Das Benutzerkonto wird im One Identity Manager gesperrt und je nach Einstellung der Löschverzögerung endgültig aus der One Identity Manager-Datenbank und aus dem Zielsystem gelöscht.

Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Um ein Benutzerkonto zu löschen, das nicht über eine Kontendefinition verwaltet wird

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.

3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .

Verwandte Themen

- Benutzerkonten deaktivieren auf Seite 124
- Löschverzögerung für Benutzerkonten der kundendefinierten Zielsysteme festlegen auf Seite 60

Überblick über Benutzerkonten anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einem Benutzerkonto.

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das Benutzerkonto**.

Gruppen in kundendefinierten Zielsystemen

Gruppen und Systemberechtigungen bilden die Objekte ab, über die im Zielsystem der Zugriff auf die Zielsystemressourcen gesteuert wird. Ein Benutzerkonto erhält über seine Mitgliedschaften in Gruppen und Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Zielsystemressourcen.

Um eine Gruppe zu erstellen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Klicken Sie in der Ergebnisliste .

3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
4. Speichern Sie die Änderungen.

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Managen der Zuweisungen von Gruppen und Systemberechtigungen auf Seite 63
- Systemberechtigungen in kundendefinierten Zielsystemen auf Seite 131
- Stammdaten für Gruppen auf Seite 127
- Gruppen an Gruppen zuweisen auf Seite 128
- Berechtigungselemente an Gruppen zuweisen auf Seite 130
- Zusatzeigenschaften an Gruppen zuweisen auf Seite 129
- Überblick über Gruppen anzeigen auf Seite 131

Stammdaten für Gruppen

Zu einer Gruppe erfassen Sie die folgenden Stammdaten.

Tabelle 27: Allgemeine Stammdaten einer Gruppe

Eigenschaft	Beschreibung
Bezeichnung	Bezeichnung der Gruppe.
Kanonischer Name	Der kanonische Name wird automatisch gebildet und sollte nicht geändert werden.
Gruppentyp	Nähere Bezeichnung des Gruppentyps.
Definierter Name	Der definierte Name wird per Bildungsregel ermittelt und sollte nicht geändert werden.
Objekt GUID	Unikale ID, unter der das Objekt im Zielsystem verwaltet wird.
Anzeigename	Name zur Anzeige der Gruppe in der Benutzeroberfläche der One Identity Manager-Werkzeuge.

Eigenschaft	Beschreibung
Zielsystem	Kennung des Zielsystems.
Container	Container, in dem die Gruppe angelegt werden soll.
Leistungsposition	Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Shop	Gibt an, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.
Mitgliedschaften nur lesbar	Gibt an, ob die Mitgliedschaften nur gelesen werden können, beispielsweise für dynamische Gruppen. Die Mitgliedschaften werden über das Zielsystem geregelt. Manuelle Änderungen der Mitgliedschaften im One Identity Manager sind nicht zulässig.

Verwandte Themen

- Vererbung von Gruppen und Systemberechtigungen anhand von Kategorien auf Seite 88
- Gruppen in den IT Shop aufnehmen auf Seite 76

Gruppen an Gruppen zuweisen

Mit dieser Aufgabe nehmen Sie eine Gruppe in andere Gruppen auf. Damit können die Gruppen hierarchisch strukturiert werden. Es können nur Gruppen zugewiesen werden, die

demselben Zielsystem angehören.

Um Gruppen als Mitglieder an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Wählen Sie den Tabreiter **Hat Mitglieder**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die untergeordneten Gruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Gruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Um eine Gruppe als Mitglied in andere Gruppen aufzunehmen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Wählen Sie den Tabreiter **Ist Mitglied in**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die übergeordneten Gruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Gruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Verwandte Themen

- Systemberechtigungen an Systemberechtigungen zuweisen auf Seite 134

Zusatzeigenschaften an Gruppen zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Ausführliche Informationen zur Einrichtung von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Um Zusatzeigenschaften für eine Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Zusatzeigenschaften entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Zusatzeigenschaft und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Zusatzeigenschaften an Systemberechtigungen zuweisen auf Seite 135

Berechtigungselemente an Gruppen zuweisen

Mit dieser Aufgabe können Sie mehrere Berechtigungselemente an eine Gruppen zuweisen.

Um Berechtigungselemente an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Berechtigungselemente zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungselemente zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Berechtigungselementen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Berechtigungselement und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Gruppen an Berechtigungselemente zuweisen auf Seite 138

Überblick über Gruppen anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Gruppe.

Um einen Überblick über eine Gruppe zu erhalten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die Gruppe**.

Systemberechtigungen in kundendefinierten Zielsystemen

Gruppen und Systemberechtigungen bilden die Objekte ab, über die im Zielsystem der Zugriff auf die Zielsystemressourcen gesteuert wird. Ein Benutzerkonto erhält über seine Mitgliedschaften in Gruppen und Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Zielsystemressourcen.

Um eine Systemberechtigung zu erstellen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Systemberechtigung.
4. Speichern Sie die Änderungen.

Um die Stammdaten einer Systemberechtigung zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

- ODER -

Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.

2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Systemberechtigung.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Managen der Zuweisungen von Gruppen und Systemberechtigungen auf Seite 63
- Gruppen in kundendefinierten Zielsystemen auf Seite 126
- Stammdaten für Systemberechtigungen auf Seite 132
- Systemberechtigungen an Systemberechtigungen zuweisen auf Seite 134
- Zusatzeigenschaften an Systemberechtigungen zuweisen auf Seite 135
- Überblick über Systemberechtigungen anzeigen auf Seite 136

Stammdaten für Systemberechtigungen

Zu einer Systemberechtigung erfassen Sie die folgenden Stammdaten.

Tabelle 28: Allgemeine Stammdaten einer Systemberechtigung

Eigenschaft	Beschreibung
Bezeichnung	Bezeichnung der Systemberechtigung.
Kanonischer Name	Der kanonische Name wird automatisch gebildet und sollte nicht geändert werden.
Typ der Systemberechtigung	Nähere Bezeichnung des Typs der Systemberechtigung.
Definierter Name	Der definierte Name wird per Bildungsregel ermittelt und sollte nicht geändert werden.
Objekt GUID	Unikale ID, unter der das Objekt im Zielsystem verwaltet wird.
Anzeigename	Anzeigename zur Anzeige der Systemberechtigung in der Benutzeroberfläche der One Identity Manager Werkzeuge.

Eigenschaft	Beschreibung
Zielsystem	Kennung des Zielsystems.
Container	Container, in dem die Systemberechtigung angelegt werden soll.
Leistungsposition	Leistungsposition, um die Systemberechtigung über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Systemberechtigung an Benutzerkonten. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Systemberechtigungen. Systemberechtigungen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Systemberechtigungen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Shop	Gibt an, ob die Systemberechtigung über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Systemberechtigung über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Systemberechtigung kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Systemberechtigung ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Systemberechtigung über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Systemberechtigung an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.
Mitgliedschaften nur lesbar	Gibt an, ob die Mitgliedschaften nur gelesen werden können, beispielsweise für dynamische Gruppen. Die Mitgliedschaften werden über das Zielsystem geregelt. Manuelle Änderungen der Mitgliedschaften im One Identity Manager sind nicht zulässig.

Verwandte Themen

- Vererbung von Gruppen und Systemberechtigungen anhand von Kategorien auf Seite 88
- Systemberechtigungen in den IT Shop aufnehmen auf Seite 78

Systemberechtigungen an Systemberechtigungen zuweisen

Systemberechtigungen können Mitglied anderer Systemberechtigungen sein. Damit können die Systemberechtigungen hierarchisch strukturiert werden. Es können nur Systemberechtigungen zugewiesen werden, die denselben Typ haben und die demselben Zielsystem angehören.

Um Systemberechtigungen als Mitglieder an eine Systemberechtigung zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Passend zur gewählten Systemberechtigung, wählen Sie die Aufgabe **Systemberechtigungen 1 zuweisen**, **Systemberechtigungen 2 zuweisen** oder **Systemberechtigungen 3 zuweisen**.
4. Wählen Sie den Tabreiter **Hat Mitglieder**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die untergeordneten Systemberechtigungen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemberechtigungen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemberechtigung und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Um eine Systemberechtigung als Mitglied in andere Systemberechtigungen aufzunehmen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.

2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Passend zur gewählten Systemberechtigung, wählen Sie die Aufgabe **Systemberechtigungen 1 zuweisen**, **Systemberechtigungen 2 zuweisen** oder **Systemberechtigungen 3 zuweisen**.
4. Wählen Sie den Tabreiter **Ist Mitglied in**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die übergeordneten Systemberechtigungen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemberechtigungen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemberechtigung und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Gruppen an Gruppen zuweisen auf Seite 128

Zusatzeigenschaften an Systemberechtigungen zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Ausführliche Informationen zur Einrichtung von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Um Zusatzeigenschaften für eine Systemberechtigung festzulegen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Zusatzeigenschaften entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Zusatzeigenschaft und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Zusatzeigenschaften an Gruppen zuweisen auf Seite 129

Überblick über Systemberechtigungen anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Systemberechtigung.

Um einen Überblick über eine Systemberechtigung zu erhalten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.

2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Passend zur gewählten Systemberechtigung, wählen Sie die Aufgabe **Überblick über Systemberechtigung 1**, **Überblick über Systemberechtigung 2** oder **Überblick über Systemberechtigung 3**.

Berechtigungselemente in kundendefinierten Zielsystemen

Berechtigungselemente nutzen Sie, um weitere Eigenschaften der Zielsysteme abzubilden. Sie können dafür die gewünschten Daten aus dem angebundenen Zielsystem in den One Identity Manager importieren. Berechtigungselemente können auch im One Identity Manager neu erstellt werden.

Um Berechtigungselemente zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste ein Berechtigungselement aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Berechtigungselements.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Stammdaten für Berechtigungselemente auf Seite 137
- Gruppen an Berechtigungselemente zuweisen auf Seite 138
- Benutzerkonten an Berechtigungselemente zuweisen auf Seite 138
- Überblick über Berechtigungselemente anzeigen auf Seite 139

Stammdaten für Berechtigungselemente

Für ein Berechtigungselement erfassen Sie die folgenden Stammdaten.

Tabelle 29: Stammdaten eines Berechtigungselements

Eigenschaft	Beschreibung
Zielsystem	Zielsystem, in dem das Berechtigungselement gültig ist.
Berechtigungselement	Bezeichnung des Berechtigungselements.
Berechtigungstyp	Zusätzliche Eigenschaft des Berechtigungselements.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Benutzerkonten an Berechtigungselemente zuweisen

Über diese Aufgabe können Sie einem Berechtigungselement mehrere Benutzerkonten zuweisen.

Um ein Berechtigungselement an Benutzerkonten zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Benutzerkonten entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Berechtigungselemente an Benutzerkonten zuweisen auf Seite 123

Gruppen an Berechtigungselemente zuweisen

Über diese Aufgabe können Sie ein Berechtigungselement an mehrere Gruppen zuweisen.

Um Gruppen an ein Berechtigungselement zuzuweisen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Gruppen entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- Berechtigungselemente an Gruppen zuweisen auf Seite 130

Überblick über Berechtigungselemente anzeigen

Auf dem Überblicksformular erhalten Sie auf einen Blick die wichtigsten Informationen zu einem Berechtigungselement.

Um einen Überblick über ein Berechtigungselement zu erhalten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > <Zielsystem> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Überblick über das Berechtigungselement**.

Berichte über kundendefinierte Zielsysteme

Der One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen Objekten der One Identity Manager-Datenbank aufbereitet sind. Für kundendefinierte Zielsysteme stehen folgende Berichte zur Verfügung.

HINWEIS: Abhängig von den vorhandenen Modulen können weitere Berichte zur Verfügung stehen.

Tabelle 30: Berichte zur Datenqualität eines Zielsystems

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Herkunft)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die Herkunft

Bericht	Bereitgestellt für	Beschreibung
		der zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Historie)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Benutzerkonten anzeigen (inklusive Historie)	Container	Der Bericht zeigt alle Benutzerkonten des Containers mit ihren Berechtigungen einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Systemberechtigungen anzeigen (inklusive Historie)	Container	Der Bericht zeigt die Systemberechtigungen des Containers mit den zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Container	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Container mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen	Systemberechtigung Gruppe	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Systemberechtigung besitzen.
Übersicht anzeigen	Systemberechtigung Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und ihre

Bericht	Bereitgestellt für	Beschreibung
		Zuweisungen.
Übersicht anzeigen (inklusive Herkunft)	Systemberechtigung Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und die Herkunft der zugewiesenen Benutzerkonten.
Übersicht anzeigen (inklusive Historie)	Systemberechtigung Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Abweichende Systemberechtigungen anzeigen	Zielsystem	Der Bericht enthält alle Systemberechtigungen, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten anzeigen (inklusive Historie)	Zielsystem	Der Bericht liefert alle Benutzerkonten mit ihren Berechtigungen einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Benutzerkonten mit einer überdurchschnittliche Anzahl an Systemberechtigungen anzeigen	Zielsystem	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen.
Personen mit mehreren Benutzerkonten anzeigen	Zielsystem	Der Bericht zeigt alle Personen, die mehrere Benutzerkonten besitzen. Der Bericht enthält eine Risikoeinschätzung.
Systemberechtigungen anzeigen (inklusive	Zielsystem	Der Bericht zeigt die Systemberechtigungen mit den

Bericht	Bereitgestellt für	Beschreibung
Historie)		zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Zielsystem	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Zielsystem mindestens ein Benutzerkonto besitzen.
Ungenutzte Benutzerkonten anzeigen	Zielsystem	Der Bericht enthält alle Benutzerkonten, die in den letzten Monaten nicht verwendet wurden.
Unverbundene Benutzerkonten anzeigen	Zielsystem	Der Bericht zeigt alle Benutzerkonten, denen keine Person zugeordnet ist.
Veränderungen an Benutzerkonten anzeigen	Zielsystem	Der Bericht zeigt für einen bestimmten Zeitraum die geänderten Benutzerkonten aller Zielsysteme an.

Verwandte Themen

- Übersicht aller Zuweisungen auf Seite 91

7

Behandeln der Objekte kundendefinierter Zielsysteme im Web Portal

Der One Identity Manager bietet seinen Benutzern die Möglichkeit, verschiedene Aufgaben unkompliziert über ein Web Portal zu erledigen.

- Managen von Benutzerkonten und Personen

  Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann die Kontendefinition von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Person, beispielsweise einen Manager, wird das Benutzerkonto angelegt.

- Managen von Zuweisungen von Gruppen und Systemberechtigungen

  Mit der Zuweisung von Gruppen und Systemberechtigungen an ein IT Shop Regal können diese Produkte von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Person wird die Gruppe oder Systemberechtigung zugewiesen.

  Manager und Administratoren von Organisationen können im Web Portal Gruppen und Systemberechtigungen an die Abteilungen, Kostenstellen oder Standorte zuweisen, für die sie verantwortlich sind. Die Gruppen und Systemberechtigungen werden an alle Personen vererbt, die Mitglied dieser Abteilungen, Kostenstellen oder Standorte sind.

  Wenn das Geschäftsrollenmodul vorhanden ist, können Manager und Administratoren von Geschäftsrollen im Web Portal Gruppen und Systemberechtigungen an die Geschäftsrollen zuweisen, für die sie verantwortlich sind. Die Gruppen und Systemberechtigungen werden an alle Personen vererbt, die Mitglied dieser Geschäftsrollen sind.

  Wenn das Systemrollenmodul vorhanden ist, können Verantwortliche von Systemrollen im Web Portal Gruppen und Systemberechtigungen an die Systemrollen zuweisen. Die Gruppen und Systemberechtigungen werden an alle Personen vererbt, denen diese Systemrollen zugewiesen sind.

- Attestierung

  Wenn das Modul Attestierung vorhanden ist, kann die Richtigkeit der Eigenschaften von Zielsystemobjekten und von Gruppenmitgliedschaften regelmäßig oder auf Anfrage bescheinigt werden. Dafür werden im Manager Attestierungsrichtlinien konfiguriert. Die Attestierer nutzen das Web Portal, um Attestierungsvorgänge zu entscheiden.

- Governance Administration

  Die Regeln werden regelmäßig und bei Änderungen an den Objekten im One Identity Manager überprüft. Complianceregeln werden im Manager definiert. Verantwortliche Personen nutzen das Web Portal, um Regelverletzungen zu überprüfen, aufzulösen und Ausnahmegenehmigungen zu erteilen.

  Wenn das Modul Unternehmensrichtlinien vorhanden ist, können Unternehmensrichtlinien für die im One Identity Manager abgebildeten Zielsystemobjekte definiert und deren Risiken bewertet werden. Unternehmensrichtlinien werden im Manager definiert. Verantwortliche Personen nutzen das Web Portal, um Richtlinienverletzungen zu überprüfen und Ausnahmegenehmigungen zu erteilen.

- Risikobewertung

  Über den Risikoindex von Gruppen kann das Risiko von Gruppenmitgliedschaften für das Unternehmen bewertet werden. Dafür stellt der One Identity Manager Standard-Berechnungsvorschriften bereit. Im Web Portal können die Berechnungsvorschriften modifiziert werden.

- Berichte und Statistiken

  Das Web Portal stellt verschiedene Berichte und Statistiken über die Personen, Benutzerkonten, deren Berechtigungen und Risiken bereit.

Ausführliche Informationen zu den genannten Themen finden Sie unter Managen von Benutzerkonten und Personen auf Seite 24, Managen der Zuweisungen von Gruppen und Systemberechtigungen auf Seite 63 und in folgenden Handbüchern:

- *One Identity Manager Web Designer Web Portal Anwenderhandbuch*
- *One Identity Manager Administrationshandbuch für Attestierungen*
- *One Identity Manager Administrationshandbuch für Complianceregeln*
- *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien*
- *One Identity Manager Administrationshandbuch für Risikobewertungen*

8

Basisdaten für kundendefinierte Zielsysteme

Für die Verwaltung eines kundendefinierten Zielsystems im One Identity Manager sind folgende Basisdaten relevant.

- Kontendefinitionen

  Um Benutzerkonten automatisch an Personen zu vergeben, kennt der One Identity Manager Kontendefinitionen. Kontendefinitionen können für jedes Zielsystem erzeugt werden. Hat eine Person noch kein Benutzerkonto in einem Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Person ein neues Benutzerkonto erzeugt.

  Weitere Informationen finden Sie unter Kontendefinitionen für Benutzerkonten auf Seite 25.

- Kennwortrichtlinien

  Der One Identity Manager unterstützt Sie beim Erstellen von komplexen Kennwortrichtlinien beispielsweise für Systembenutzerkennwörter, das zentrale Kennwort von Personen sowie für Kennwörter für die einzelnen Zielsysteme. Kennwortrichtlinien werden sowohl bei der Eingabe eines Kennwortes durch den Anwender als auch bei der Generierung von Zufallskennwörtern angewendet.

  In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können. Zusätzlich können Sie eigene Kennwortrichtlinien definieren.

  Weitere Informationen finden Sie unter Kennwortrichtlinien für Benutzerkonten auf Seite 93.

- Initiales Kennwort für neue Benutzerkonten

  Um das initiale Kennwort für Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Tragen Sie beim Erstellen eines Benutzerkontos ein Kennwort ein oder verwenden Sie ein zufällig generiertes initiales Kennwort.

  Weitere Informationen finden Sie unter Initiales Kennwort für neue Benutzerkonten auf Seite 105.

- E-Mail-Benachrichtigungen über die Anmeldeinformationen

Bei Erstellung eines neuen Benutzerkontos werden die Anmeldeinformationen an definierte Empfänger versendet. Dabei werden zwei Benachrichtigungen versendet, die den Benutzernamen und das initiale Kennwort enthalten. Zur Erzeugung der Benachrichtigungen werden Mailvorlagen genutzt.

Weitere Informationen finden Sie unter E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 106.

- Server

  Für die Provisionierung der Daten aus dem One Identity Manager in ein kundendefiniertes Zielsystem über die Synchronisation per Skript muss ein Server bereitgestellt werden, auf dem der One Identity Manager Service installiert, konfiguriert und gestartet ist. Der Server muss im One Identity Manager bekannt sein und am Zielsystem als Synchronisationsserver eingetragen werden.

  Weitere Informationen finden Sie unter Jobserver für die Provisionierung der Daten in ein kundendefiniertes Zielsystem auf Seite 14.

- Zielsystemverantwortliche

  Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, alle Zielsysteme im One Identity Manager zu bearbeiten.

  Wenn Sie die Berechtigungen der Zielsystemverantwortlichen auf einzelne Zielsysteme einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

  Weitere Informationen finden Sie unter Zielsystemverantwortliche auf Seite 147.

- Zielsystemtypen

  Über einen Zielsystemtyp können mehrere Zielsysteme zusammengefasst werden. Je nach Konfiguration des Zielsystemtyps, können Gruppen und Systemberechtigungen an Benutzerkonten auch dann zugewiesen, wenn diese verschiedenen Zielsystemen angehören. Zielsystemtypen werden für die Konfiguration des Zielsystemabgleichs benötigt. An den Zielsystemtypen werden die Tabellen gepflegt, die ausstehende Objekte enthalten können. Es werden Einstellungen für die Provisionierung von Mitgliedschaften und die Einzelobjektsynchronisation vorgenommen. Zusätzlich dient der Zielsystemtyp zur Abbildung der Objekte im Unified Namespace.

  Weitere Informationen finden Sie unter Zielsystemtypen für kundendefinierte Zielsysteme auf Seite 149.

- Kundenspezifische Schemaerweiterungen an den Basistabellen

  Kundenspezifische Spalten an den Tabellen `UNSAccountB`, `UNSContainerB`, `UNSGroupB`, `UNSGroupB1`, `UNSGroupB2`, `UNSGroupB3`, `UNSItemB` und `UNSRootB` können Sie auf den Formularen im Manager anzeigen. Dazu passen Sie die Spaltendefinition der kundenspezifischen Spalten an.

  Weitere Informationen finden Sie unter Anzeige kundenspezifischer Schemaerweiterungen für kundendefinierte Zielsysteme konfigurieren auf Seite 151.

Zielsystemverantwortliche

Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, alle Zielsysteme im One Identity Manager zu bearbeiten.

Wenn Sie die Berechtigungen der Zielsystemverantwortlichen auf einzelne Zielsysteme einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

Ausführliche Informationen zum Einsatz und zur Bearbeitung von Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

1. Der One Identity Manager Administrator legt Personen als Zielsystemadministratoren fest.
2. Die Zielsystemadministratoren nehmen die Personen in die Standardanwendungsrolle für die Zielsystemverantwortlichen auf.

   Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle Zielsysteme im One Identity Manager zu bearbeiten.
3. Zielsystemverantwortliche können innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche berechtigen und bei Bedarf weitere untergeordnete Anwendungsrollen erstellen und einzelnen Zielsystemen zuweisen.

Tabelle 31: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Kundendefinierte Zielsysteme** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen und Systemberechtigungen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den

Benutzer	Aufgaben
	Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Um initial Personen als Zielsystemadministrator festzulegen

1. Melden Sie sich als One Identity Manager Administrator (Anwendungsrolle **Basisrollen | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration > Zielsysteme > Administratoren**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Person zu und speichern Sie die Änderung.

Um initial Personen in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen

1. Melden Sie sich als Zielsystemadministrator (Anwendungsrolle **Zielsysteme | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration > Zielsysteme > Kundendefinierte Zielsysteme**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Um als Zielsystemverantwortlicher weitere Personen als Zielsystemverantwortliche zu berechtigen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie in der Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Zielsystemverantwortliche** die Anwendungsrolle.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Um Zielsystemverantwortliche für einzelne Zielsysteme festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Zielsysteme**.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

4. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Zielsystemverantwortliche** die Anwendungsrolle.

   - ODER -

   Klicken Sie neben der Auswahlliste **Zielsystemverantwortliche** auf , um eine neue Anwendungsrolle zu erstellen.

   a. Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | Kundendefinierte Zielsysteme** zu.

   b. Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.
5. Speichern Sie die Änderungen.
6. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, das Zielsystem im One Identity Manager zu bearbeiten.

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung von kundendefinierten Zielsystemen auf Seite 8
- Allgemeine Stammdaten für kundendefinierte Zielsysteme auf Seite 110

Zielsystemtypen für kundendefinierte Zielsysteme

Über einen Zielsystemtyp können mehrere Zielsysteme zusammengefasst werden. Je nach Konfiguration des Zielsystemtyps, können Gruppen und Systemberechtigungen an Benutzerkonten auch dann zugewiesen, wenn diese verschiedenen Zielsystemen angehören. Zielsystemtypen werden für die Konfiguration des Zielsystemabgleichs benötigt. An den Zielsystemtypen werden die Tabellen gepflegt, die ausstehende Objekte enthalten können. Es werden Einstellungen für die Provisionierung von Mitgliedschaften und die Einzelobjektsynchronisation vorgenommen. Zusätzlich dient der Zielsystemtyp zur Abbildung der Objekte im Unified Namespace.

Um einen Zielsystemtyp zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp.

   - ODER -

   Klicken Sie in der Ergebnisliste .

3. Bearbeiten Sie die Stammdaten des Zielsystemtyps.

Tabelle 32: Stammdaten eines Zielsystemtyps

Eigenschaft	Beschreibung
Zielsystemtyp	Bezeichnung des Zielsystemtyps.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Anzeigename	Name des Zielsystemtyps zur Anzeige in den One Identity Manager-Werkzeugen.
Grenzüberschreitende Vererbung	Angabe zur Zuweisung und Vererbung von Gruppen und Systemberechtigungen an Benutzerkonten, wenn diese verschiedenen kundendefinierten Zielsystemen angehören. • Ist die Option aktiviert, können Gruppen und Systemberechtigungen an Benutzerkonten zugewiesen werden, die zum selben Zielsystem oder zu unterschiedlichen Zielsystemen gehören. Die Zielsysteme müssen zum selben Zielsystemtyp gehören. Für alle Zielsysteme eines Zielsystemtyps müssen die Einstellungen für die Spalte **Benutzerkonto enthält Mitgliedschaften** (`UNSRootB.UserContainsGroupList`) identisch sein. • Ist die Option deaktiviert, können Gruppen und Systemberechtigungen nur an Benutzerkonten desselben Zielsystems zugewiesen werden. HINWEIS: Ist die Option nicht gesetzt, kann der Zielsystemtyp zur einfachen Gruppierung der Zielsysteme verwendet werden.
Anzeige im Regeleditor für Complianceregeln	Gibt an, ob der Zielsystemtyp im Regeleditor für Complianceregeln beim Erstellen von Regelbedingungen ausgewählt werden kann.
Textbaustein	Textbaustein, der zum Verketten der Texte im Regeleditor für Complianceregeln verwendet wird.
Alternative Konnektoren	Liste von Konnektoren, welche diesen Zielsystemtyp ebenfalls verarbeiten können.

4. Speichern Sie die Änderungen.

Um einem kundendefinierten Zielsystem einen Zielsystemtyp zuzuordnen

1. Wählen Sie im Manager die Kategorie **Kundendefinierte Zielsysteme > Basisdaten zur Konfiguration > Zielsystem**.

2. Wählen Sie in der Ergebnisliste das Zielsystem.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie aus der Auswahlliste **Zielsystemtyp** den Zielsystemtyp aus, dem das Zielsystem zugeordnet werden soll.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Zuweisen von Gruppen und Systemberechtigungen an Benutzerkonten im One Identity Manager auf Seite 66
- Nachbehandlung ausstehender Objekte auf Seite 19
- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 20

Anzeige kundenspezifischer Schemaerweiterungen für kundendefinierte Zielsysteme konfigurieren

Kundenspezifische Spalten an den Tabellen `UNSAccountB`, `UNSContainerB`, `UNSGroupB`, `UNSGroupB1`, `UNSGroupB2`, `UNSGroupB3`, `UNSItemB` und `UNSRootB` können Sie auf den Formularen im Manager anzeigen. Dazu passen Sie die Spaltendefinition der kundenspezifischen Spalten an.

Ausführliche Informationen zur Erweiterung von Tabellen um kundenspezifische Spalten mit dem Programm Schema Extension und zum Anpassen der Spaltendefinitionen mit dem Designer finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um kundenspezifische Spalten an den Tabellen UNSAccountB, UNSContainerB, UNSGroupB, UNSGroupB1, UNSGroupB2, UNSGroupB3, UNSItemB und UNSRootB auf den Formularen im Manager anzuzeigen

- Legen Sie im Designer in der Eigenschaft **Reihenfolge** (`DialogColumn.SortOrder`) die Anzeigereihenfolge der Eingabefelder fest. Spalten, deren Reihenfolge kleiner eins ist, werden nicht angezeigt.
- Passen Sie im Designer die Eigenschaft **Gruppe** (`DialogColumn.ColumnGroup`) in der Spaltendefinition der kundenspezifischen Spalten an. Die Gruppe entscheidet, auf welchem Tabreiter die Spalten angezeigt werden.
    - Wenn Sie in der Spaltenkonfiguration keine Gruppe angeben, dann wird die Spalte für alle Zielsystemtypen auf einem Tabreiter mit der Bezeichnung **Kundenspezifisch** angezeigt.

- Wenn Sie in der Spaltenkonfiguration eine Gruppe eintragen, dann wird die Spalte für alle Zielsystemtypen auf einem Tabreiter mit der Bezeichnung der Gruppe angezeigt. Die Bezeichnung der Gruppe darf dabei nicht der Bezeichnung eines Zielsystemtyps entsprechen.
- Um eine Spalte nur für einen bestimmten Zielsystemtyp anzuzeigen, tragen Sie nur diesen Zielsystemtyp (`DPRNamespace.Ident_DPRNamespace`) als Gruppe ein. Die Spalte wird auf einem Tabreiter mit der Bezeichnung des Zielsystemtyps angezeigt. Für alle anderen Zielsystemtypen wird diese Spalte nicht angezeigt.
- Um eine Spalte für mehrere Zielsystemtypen anzuzeigen, tragen Sie diese Zielsystemtypen mit Komma (,) getrennt als Gruppen ein. Die Spalte wird je eingetragenem Zielsystemtyp auf einem Tabreiter mit der Bezeichnung des Zielsystemtyps angezeigt. Für alle anderen Zielsystemtypen wird diese Spalte nicht angezeigt.
- Um die Spalte für einen oder mehrere Zielsystemtypen anzuzeigen, jedoch auf einem Tabreiter mit einer anderen Bezeichnung, tragen Sie die Zielsystemtypen mit Komma (,) getrennt und die Bezeichnung des Tabreiters als Gruppe ein. Diese Gruppe wird als Tabreiterbezeichnung für alle eingetragenen Zielsystemtypen verwendet. Für alle anderen Zielsystemtypen wird diese Spalte nicht angezeigt.

Beispiel:

Die Tabelle `UNSAccountB` wird um 5 Spalten erweitert. Die Spalten sollen für Zielsystemtyp A, Zielsystemtyp B und Zielsystemtyp C folgendermaßen angezeigt werden.

- Die Spalte 1 soll für alle Zielsystemtypen auf dem Tabreiter **Kundenspezifisch** angezeigt werden.
- Die Spalte 2 soll für alle Zielsystemtypen auf dem Tabreiter **Gruppe A** angezeigt werden.
- Die Spalte 3 soll für Zielsystemtyp B auf dem Tabreiter **Zielsystemtyp B** angezeigt werden. Für Zielsystemtyp A und Zielsystemtyp C soll die Spalte nicht angezeigt werden.
- Die Spalte 4 soll für Zielsystemtyp B auf dem Tabreiter **Zielsystemtyp B** und für Zielsystemtyp C auf dem Tabreiter **Zielsystemtyp C** angezeigt werden. Für Zielsystemtyp A soll die Spalte nicht angezeigt werden.
- Die Spalte 5 soll für Zielsystemtyp B und für Zielsystemtyp C auf dem Tabreiter **Gruppe A** angezeigt werden. Für Zielsystemtyp A soll die Spalte nicht angezeigt werden.

Tabelle 33: Beispiel der Spaltenkonfiguration

Spalte	Gruppe
Spalte 1	
Spalte 2	Gruppe A
Spalte 3	Zielsystemtyp B
Spalte 4	Zielsystemtyp B, Zielsystemtyp C
Spalte 5	Zielsystemtyp B, Zielsystemtyp C, Gruppe A

Anhang A

Konfigurationsparameter für die Verwaltung kundendefinierter Zielsysteme

Mit der Installation des Moduls sind zusätzlich folgende Konfigurationsparameter im One Identity Manager verfügbar.

Tabelle 34: Konfigurationsparameter für die Verwaltung kundendefinierter Zielsysteme

Konfigurationsparameter	Bedeutung
TargetSystem | UNS	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung kundendefinierter Zielsysteme. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
TargetSystem | UNS | Accounts	Erlaubt die Konfiguration der Angaben zu Benutzerkonten.
TargetSystem | UNS | Accounts | InitialRandomPassword	Legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in den Konfigurationsparametern unterhalb gesetzt sind.
TargetSystem | UNS | Accounts | InitialRandomPassword	Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Geschäftsrolle,

Konfigurationsparameter	Bedeutung
| SendTo	Verantwortlicher der Person oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter **TargetSystem | UNS | DefaultAddress** hinterlegte Adresse versandt.
TargetSystem | UNS | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto** verwendet.
TargetSystem | UNS | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** verwendet.
TargetSystem | UNS | Accounts | MailTemplateDefaultValues	Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | UNS | CreateNewRoot	Legt fest, ob neue Zielsysteme angelegt werden können. Ist der Parameter aktiviert, können kundendefinierte Zielsysteme angelegt werden. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
TargetSystem | UNS | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | UNS | MaxFullsyncDuration	Maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.

Konfi-gurationsparameter	Bedeutung
TargetSystem | UNS | PersonAutoDefault	Modus für die automatische Personenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | UNS | PersonAu-toDisabledAccounts	Legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem | UNS | PersonAutoFullSync	Modus für die automatische Personenzuordnung für Benutzerkonten, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem | UNS | PersonExcludeList	Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.* |SUPPORT_.*|.* | $`

Über uns

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie https://www.oneidentity.com/company/contact-us.aspx.

Technische Supportressourcen

Technische Unterstützung steht für One Identity Kunden mit einem gültigen Wartungsvertrag und Kunden mit Testversionen zur Verfügung. Sie können auf das Support Portal unter https://support.oneidentity.com/ zugreifen.

Das Support Portal bietet Selbsthilfe-Tools, die Sie verwenden können, um Probleme schnell und unabhängig zu lösen, 24 Stunden am Tag, 365 Tage im Jahr. Das Support Portal ermöglicht Ihnen:

- Senden und Verwalten von Serviceanfragen
- Anzeigen von Knowledge Base Artikeln
- Anmeldung für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Videos unter www.YouTube.com/OneIdentity
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

Index

O

P

S

Z